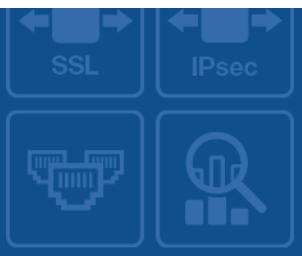
FORTINET
High Performance Network Security

FortiOS™ Handbook - What's New

VERSION 5.4.6



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

Thursday, January 11, 2018

FortiOS™ Handbook - What's New

01-543-117003-20170104

TABLE OF CONTENTS

Change Log

Date	Change Description
January 11, 2018	Update to System section.
October 23, 2017	Updated for FortiOS 5.4.6.
October 3, 2017	Corrected the comparability information in Managed FortiSwitch on page 53.
August 21, 2017	Cover version subtitle changed to match current version of the firmware. Corrected typo. Note snippet added to explain that no new features were added in 5.4.5.
August 4, 2017	Added RFC 4787 to RFCs supported by FortiOS 5.4 on page 165.
April 12, 2017	Correction to Security Profiles table mapping features to inspection modes in Changing the FortiGate's inspection mode to flow or proxy.
February 22, 2016	Correction to "Improve dynamic routing event logging (231511)" and Misc. other fixes.
February 10, 2016	What's New in FortiOS 5.4.4.
February 6, 2017	Improvements and corrections to Bootstrapping enabled for FortiGate VM platforms (391527) on page 26.
January 20, 2017	Added Bootstrapping enabled for FortiGate VM platforms (391527) on page 26.
January 4, 2017	What's New in FortiOS 5.4.3.
December 28, 2016	Typos and other minor errors fixed throughout.
October 28, 2016	What's New in FortiOS 5.4.2.
Sep 27, 2016	Correction to CLI in Changing the FortiGate's inspection mode to flow or proxy.
Aug 31, 2016	Updated "VDOMs" on page 201.
August 26, 2016	Changed presentation of Security Profile features in different inspection modes from lists to comparative table and added detail on setting inspection mode when VDOMs are enabled.
July 27, 2016	Clarification of Mobile Malware mantis bug 288022 and changes to subscription for Botnet / IP Reputation database.
July 19, 2016	Minor fix to full name for GARP.

Date	Change Description
June 21, 2016	Added information about WAN Optimization support in Changing the FortiGate's inspection mode to flow or proxy on page 60 and WAN Optimization on page 203.
June 17, 2016	Added information about VDOM support and compatibility with CSF.
June 15, 2016	Misc fixes. Additional information added to the FortiClient Profiles content in Security Profiles on page 167.
June 6, 2016	What's New in 5.4.1.
April 22, 2016	Minor changes throughout the document.
March 22, 2016	Updates to SSL VPN on page 185 re: web portal CLI syntax.
February 23, 2016	More information added to VDOMs on page 201 about the stackable VDOM licenses feature.
February 17, 2016	Updates to WAN Optimization on page 203.
January 22, 2016	Changes to DLP changes (297960) on page 172, External Security Devices on page 1, and Hardware acceleration on page 125. Web Application Firewall content moved into External Security Devices chapter. Other fixes.
January 15, 2016	Fixes and changes throughout the document.
December 30, 2015	Added a new section about enabling FortiHeartBeat for interfaces in Networking on page 151
December 22, 2015	Second set of changes. Changes to FortiSandbox Integration on page 72, Authentication on page 93, and WiFi on page 206.
December 22, 2015	Changes to External Security Devices on page 1, System on page 188, WAN Optimization on page 203
December 17, 2015	Initial release.

Introduction

This document highlights and describes many of the new features in FortiOS 5.4. Most new feature descriptions include a feature number that references the internal Fortinet ID used to track the feature.

How this guide is organized

This FortiOS Handbook chapter contains the following sections.

What's New in FortiOS 5.4.6 provides a brief description of features that were added to FortiOS 5.4.6.

What's New in FortiOS 5.4.4 provides a brief description of features that were added to FortiOS 5.4.4.

What's New in FortiOS 5.4.3 provides a brief description of features that were added to FortiOS 5.4.3.

What's New in FortiOS 5.4.2 provides a brief description of features that were added to FortiOS 5.4.2.

There is no What's New in FortiOS 5.4.5 because there were no new features added in that version.

The following sections highlight some of the higher profile new FortiOS 5.4 features:

- Cooperative Security Fabric (CSF)
- Policy Learning Mode
- FortiView
- Cloud Access Security Inspection (CASI)
- Managed FortiSwitch
- Changing the FortiGate's inspection mode to flow or proxy
- GUI Refresh
- DNS Filter
- FortiSandbox Integration
- Traffic Shaping Policies
- WAN link load balancing
- Virtual Wire Pair

All of the other new features in FortiOS 5.4 are organized alphabetically by subject:

- Authentication
- PCI DSS compliance
- Device identification
- Diagnose command changes
- Explicit web proxy
- Firewall

- FortiGate VM
- Hardware acceleration
- High Availability
- IPsec VPN
- IPv6
- Load balancing
- Logging and Reporting
- Maximum values changes
- Networking
- RFCs supported by FortiOS 5.4
- Security Profiles
- Session-aware Load Balancing (SLBC)
- SSL VPN
- System
- VDOMs
- WAN Optimization
- WiFi

What's New in FortiOS 5.4.6

Most development work in FortiOS 5.4.6 involved resolving issues. However, the following new features were added as well.

User group authentication timeout range increased to 30 days (378085)

The user authentication timeout for users in a user group has been extended to 30 days.

```
config user group
   edit <group-name>
      set authtimeout 43200
   end
```

Where `authtimeout` is the length of the timeout in minutes. An `authtimeout` of 43200 minutes is equivalent to 30 days. Set `authtimeout` to 0 to use the default authentication timeout.

FortiOS-VM support 10 interfaces (397860)

New installations of FortiOS-VM for FortiOS 5.4.6 now include 10 interfaces.

Improved support for RFCs 5746 and 7627 (422133)

FortiOS includes improved support of RFC 5746 : TLS Renegotiation Indication Extension and RFC 7627: TLS Session Hash and Extended Master Secret Extension.

Stripping clear text padding and IPsec session ESP padding (416950)

In some situations, when clear text or ESP packets in IPsec sessions may have large amounts of layer 2 padding, the NP6 IPsec engine may not be able to process them and the session may be blocked.

If you notice dropped IPsec sessions, you could try using the following CLI options to cause the NP6 processor to strip clear text padding and ESP padding before sending the packets to the IPsec engine. With padding stripped, the session can be processed normally by the IPsec engine.

Use the following command to strip ESP padding:

```
config system npu
   set strip-esp-padding enable
   set strip-clear-text-padding enable
end
```

Stripping clear text and ESP padding are both disabled by default.

Optionally disable NP6 offloading of traffic passing between 10Gbps and 1Gbps interfaces (392436)

Due to NP6 internal packet buffer limitations, some offloaded packets received at a 10Gbps interface and destined for a 1Gbps interface can be dropped, reducing performance for TCP and IP tunnel traffic. If you experience this performance reduction, you can use the following command to disable offloading sessions passing from 10Gbps interfaces to 1Gbps interfaces:

```
config system npu
   set host-shortcut-mode host-shortcut
end
```

Select `host-shortcut` to stop offloading TCP and IP tunnel packets passing from 10Gbps interfaces to 1Gbps interfaces. TCP and IP tunnel packets passing from 1Gbps interfaces to 10Gbps interfaces are still offloaded as normal.

If `host-shortcut` is set to the default `bi-directional` setting, packets in both directions are offloaded.

BFD echo mode support (enable/disable blocking land attacks) (441740)

A new option has been added to FortiOS 5.4.6 that allows you to enable or disable blocking land attacks:

```
config system settings
   set block-land-attack {disable | enable}
end
```

This option is disabled by default. Since its a `system settings` option you can enable or disable blocking land attacks for individual VDOMs if your FortiGate is operating with multiple VDOMs.

Another reason to enable this feature would be if your FortiGate is blocking BFD echo packets that should be allowed to pass through the FortiGate. For example, a FortiGate operating in Transparent mode between two routers with a policy that allows all traffic may block BFD echo communication between the routers if blocking land attacks is disabled.

Enabling blocking land attacks allows BFD echo packets to pass through the FortiGate. Use the following command to block land attacks and allow BFD echo packets.

```
config system settings
   set block-land-attack enable
end
```

Memory compatibility mode for HA between FortiGates of different hardware generations (436585)

Different hardware generations of some FortiGate models may have different amounts of system memory. In HA mode this means the primary unit, if it has more memory than the backup unit, could be able to handle more sessions than the backup unit. So after a failover some sessions could be lost if the backup unit doesn't have enough memory for all of the sessions. If you have a cluster of FortiGates from different hardware generations you can use the following command to enable memory compatibility mode to prevent session loss after a failover. Memory compatibility mode is disabled by default.

```
config system ha
   set memory-compatible-mode {disable | enable}
end
```

Memory compatibility mode synchronizes the memory size among the units in the cluster. The amount of memory available on the FortiGate with the lowest amount of memory is set as the soft total memory for each FortiGate in the cluster. That way, after a failover the new primary unit will have the same amount of memory for processing sessions and will support the same number of sessions as the former primary unit. As a result, after a failover no sessions are lost.

WiFi split tunnel enhancement (413142)

In a WTP profile, you can use the following command to control whether packets that match the split tunneling access control list (ACL) use the CAPWAP tunnel or the local LAN between the FortiAP and the FortiGate.

```
config wireless-controller wtp-profile
   edit <profile-name>
      set split-tunneling-acl-path {tunnel | local}
   end
```

where:

`tunnel` packets from wireless clients that match the split tunneling ACL pass from the FortiAP through the CAPWAP tunnel to the FortiGate (tunnel mode) and then to their destination.

`local` (the default) packets from wireless clients that match the split tunneling ACL pass across the local LAN from the FortiAP to the FortiGate (source NAT applied) and then to their destination.

What's New in FortiOS 5.4.4

Most development work in FortiOS 5.4.4 involved resolving issues. However, there was a new feature as well.

Configure the number of IPsec engines NP6 processors use (370586)

NP6 processors use multiple IPsec engines to acceleration IPsec encryption and decryption. In some cases out of order ESP packets can cause problems if multiple IPsec engines are running. To resolve this problem you can configure all of the NP6 processors to use fewer IPsec engines.

Use the following command to change the number of IPsec engines used for decryption (`ipsec-dec-subengine-mask`) and encryption (`ipsec-enc-subengine-mask`). These settings are applied to all of the NP6 processors in the FortiGate unit.

```
config system npu
   set ipsec-dec-subengine-mask <engine-mask>
   set ipsec-enc-subengine-mask <engine-mask>
end
```

`<engine-mask>` is a hexadecimal number in the range 0x01 to 0xff where each bit represents one IPsec engine. The default `<engine-mask>` for both options is 0xff which means all IPsec engines are used. Add a lower `<engine-mask>` to use fewer engines. You can configure different engine masks for encryption and decryption.

What's New in FortiOS 5.4.3

Most development work in FortiOS 5.4.3 involved resolving issues. However, there was a new feature as well.

FortiGate compatibility with FortiAP-C series (380150, 386116, 383004)

A new command, `fapc-compatibility` under `config wireless-controller setting`, has been added to enable or disable FortiAP-C series management by the FortiGate. Default FortiAP-C wtp-profiles will be added once the command is enabled.

This feature is only available when the command's `country` setting is set to either `CN` (China) or `SG` (Singapore); all other countries are unsupported. This options is disabled by default.

To enable FortiGate compatibility with FortiAP-C, enter the following command:

```
config wireless-controller setting
   set country {CN | SG}
   set fapc-compatibility {enable | disable}
end
```

Note that disabling `fapc-compatibility` will remove all the FAP-C series `wtp-groups`, `wtps`, and `wtp-profiles`.

FortiAP-C series models will become available as supported platform types under `config wireless-controller wtp-profile`, but only when `country` in `wireless-controller setting` and `ap-country` in `wtp-profile` are both set to the same supported country (either China or Singapore).

The following FortiAP-C models are supported platform models for this command: C220C, C225C, C221E, C226E, C23JD, C24JE, and C21D.

To set the platform type, enter the following command:

```
config wireless-controller wtp-profile
   edit <example>
      config platform
         set type <model>
      end
end
```

What's New in FortiOS 5.4.2

Most development work in FortiOS 5.4.2 involved resolving issues. However, there were a few new features as well.

Bootstrapping enabled for FortiGate VM platforms (391527)

All FortiOS 5.4.2 VM platforms support bootstrapping, allowing you to setup an iso file package that simplifies deploying FortiOS VMs. Using bootstrapping you can create a package that includes the VM firmware, a network configuration customized for your network and VM licensing, and other configuration elements such as basic firewall policies. You can then use the iso file to deploy FortiOS VM firmware into your VM environment.

To set up bootstrapping you need a VM license file and a default FortiOS VM configuration file. The configuration file sets up default FortiOS VM settings such as adding a hostname, configuring interfaces and so on.

Components of the config file should be similar to the following:

```
#---------configfirewall.conf-----------
root@KVM-Hypervisor:~/vz-wip# cat FGT_CONFIG_DRIVE/openstack/latest/user_data
#VM Config File
config system global
   set hostname vFGTvm00
end
config system interface
   edit port1
      set alias "EXT"
      set description "Management Network (DHCP) eth0br"
      set allowaccess ping https ssh fgfm
      set mode dhcp
   next
   edit port2
      set alias "Internal"
      set description "Liveliness Network (Static) gluebr0"
      set allowaccess ping https ssh fgfm
      set ip 192.168.1.10/24
   next

config firewall policy
   edit 0
      set name "Allow any any"
      set srcintf "port2"
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set nat enable
   next
end

config sys dns
   set primary 8.8.8.8
```

```
   unset secondary
end

config sys global
   set hostname fgt-vm-workshop
end
```

Then create a configuration file used to build the iso file, for example:

```
{
"bucket" : "confftnt",
"region" : "us-west-2",
"license" : "/FGVM080000066848.lic",
"config" : "/configfirewall.conf",
}
```

ISO Structure

It is also important that the ISO have similar structure and permissions to the following:

The user account of the intaller has been replaced with `<user_account>`.

```
<user_account>:iso <user_account>$ ll -R
total 8
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 15:14 .
drwxr-xr-x@ 8 root wheel 272 Jan 23 10:07 ..
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:53 openstack
.
.
.

./openstack:
total 16
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:53 .
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 15:14 ..
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:53 content
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:54 latest
.
.
.

./openstack/content:
total 12
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:53 .
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:53 ..
-rwxr-xr-x 1 <user_account> staff 287 Jan 19 16:02 0000
.
.
.
./openstack/latest:
total 12
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:54 .
drwxr-xr-x 1 <user_account> staff 2048 Jan 20 14:53 ..
-rwxr-xr-x 1 <user_account> staff 813 Jan 19 16:02 user_data
.
.
.
```

Where “0000” has the following content:

```
<user_account>:iso <user_account>$ cat openstack/content/0000
-----BEGIN FGT VM LICENSE-----
QAAAAFS1V9CLl8h69qtDbikc4yW8hSi0kyFBlFi1LqQlqXG59uCLSlJiGfHt6ddbweM0d3guoeu
uzPLA/AjPJ3/4bdgAAAAQe5bBXvK4/UTEHyCP1VFL7OUHn/84246+gFHw75lYi5Pae3PmSmlR3E
AB7kRpLJFa+A5GpCKBu2sXKWwgQGZFmHbLOT7c5HO7BbPNo8Og0oR1b/YUtnCB22mXCXp1yY
-----END FGT VM LICENSE-----
```

FortiAP-421E and 423E and wave 2 WiFi support (371374)

FortiOS 5.4.2 includes FortiAP profiles for the FortiAP-421E and FortiAP-423E and these profiles include support for Wave 2 WiFi.

Dynamic Frequency Selection (DFS) support added (369052)

DFS support has been added for FortiAP models that support it. FortiAP models that support this feature include the 321C, 323C, 421E, S421E, 423E, S423E, and S422E.

BGP local-AS support (307530)

Use the following command to configure BGP local-AS support:

```
config router bgp
   config neighbor
      edit "neighbor"
         ...
         set local-as 300
         set local-as-no-prepend disable|enable
         set local-as-replace-as disable|enable
      end
```

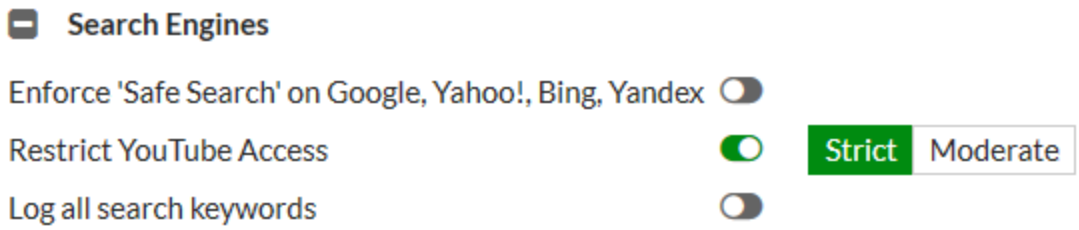
Enable `local-as-no-prepend` if you do not want to prepend local-as to incoming updates.

Enable `local-as-replace-as` to replace a real AS with local AS in outgoing updates.

Restricting access to YouTube (replacement for the YouTube Education filter feature) (378277)

Previous versions of FortiOS supported YouTube for Schools (YTfS). As of July 1, 2016 this feature is no longer supported by YouTube. Instead you can use the information in the YouTube support article Restrict YouTube content on your network or managed devices to achieve the same result. FortiOS supports applying **Strict** or **Moderate** restrictions using HTTP headers as described in this article.

In FortiOS 5.4.2 with inspection mode set to proxy-based, in a Web Filter profile under **Search Engines** you can select **Restrict YouTube Access** and select either **Strict** or **Moderate**.



High Availability hello-holddown CLI option typo fix (382364)

The `config system ha` option `helo-holddown` has been renamed `hello-holddown`.

DNS filter available in flow mode (390957)

DNS filter security profiles can now be edited and added to security policies if the FortiGate or the current VDOM Inspection Mode is set to Flow-based.

Patch apache server vulnerabilities (379870)

The following CLI commands have been added as part of an update to protect SSL VPN connections to the FortiGate from Slowloris (CVE-2007-6750) and R-U-Dead-Yet attacks.

```
config vpn ssl settings
   set http-request-header-timeout 20
   set http-request-body timeout 30
end
```

`http-request-header-timeout` protects against Slowloris by controlling maximum time to read the HTTP request header. If the HTTP header does not complete within this time, SSL VPN disconnects the connection with response code 408 (Request Timeout). The default is 20 seconds and the range is 1 to 60 seconds.

`http-request-body-timeout` protects against R-U-Dead-Yet attacks by controlling the maximum time to read a HTTP request body. If the HTTP body does not complete within this time, SSL VPN disconnects the connection with response code 408 (Request Timeout). The default is 30 seconds and the range is 1 to 60 seconds.

Diagnose hardware test added to select FortiGate models (388646 302021 381208)

Most current FortiGate models include the `diagnose hardware test` command that you can use to test all aspects of a FortiGate's hardware and report on problems that are found.

Antispam log message improvements (284055)

When Antispam protection finds a phishing URL in an email message, the log message recorded for this event now includes the phishing URL found in the email message. The phishing URL is included in the `fortiguardresp` log message field.

Last session information saved in a crash log when an IPS engine crash occurs (378252)

Changes to FortiOS IPS and to the IPS engine version 3.170 now cause FortiOS to save a crash log with the last session information when an IPS crash occurs. This information can be used by Fortinet support to diagnose the cause of the crash.

Cooperative Security Fabric (CSF)

In FortiOS 5.4.1, new features were added allowing a FortiGate to be configured as part of a Cooperative Security Fabric (CSF). A CSF links different security sensors and tools together in order to collect, coordinate, and respond to malicious behavior anywhere it occurs in real time.

Multiple VDOM support is disabled when CSF is enabled.

Fortinet Cookbook Recipe Collection

To demonstrate how to configure a CSF, the Cooperative Security Fabric collection has been published on the Fortinet Cookbook website. This collection will be added to over time, so check back to see if anything new has been added.

Cooperative Security Fabric Menu

The Cooperative Security Fabric menu can be found at **System > Cooperative Security Fabric**. From here you can enable CSF on the FortiGate and, if necessary, configure the FortiGate to connect to an upstream FortiGate.

CSF FortiView Dashboards

Two new FortiView dashboards have been added to display information about a CSF. The **Physical Topology** dashboard shows all access layer devices, while the **Logical Topology** dashboard displays information about the interface (logical or physical) that each device is connected to.

FortiTelemetry

FortiTelemetry is a protocol, similar to the FGCP heartbeat, used for communication between different Fortinet products. It is used to connect devices in a CSF, to support On-Net functionality, and monitor and enforce FortiClient use for devices on a network protected by FortiOS.

FortiTelemetry must be enabled on interfaces that connect devices in the CSF.

External Security Devices

External Security Devices can be configured as means to offload processes to other devices, such as a FortiWeb, FortiCache, or FortiMail. Example processes could include HTTP inspection, web caching, and anti- spam.

Offloading HTTP traffic to FortiWeb

Use the following steps to offload HTTP traffic to FortiWeb to apply Web Application Firewall features to the traffic. Using these steps you can select the HTTP traffic to offload by adding a web application firewall profile configured for external inspection to selected firewall policies. Only the HTTP traffic accepted by those firewall policies is offloaded.

If you offload HTTP traffic to FortiWeb you can also apply other HTTP inspection to it from your FortiGate including virus scanning and web filtering.

A single FortiGate cannot offload HTTP traffic to both FortiCache and FortiWeb.

To offload HTTP traffic to FortiWeb:

1. Go to the **System Information** dashboard widget and make sure **Inspection Mode** is set to **Proxy-based**.
2. Go to **System > Feature Select** and turn on **Web Application Firewall**.
3. Go to **System > Cooperative Security Fabric**, enable **HTTP Service**, select **FortiWeb** and add the IP addresses of your FortiWeb devices. You can also select **Authentication** add a **password** if required.
4. Go to **Security Profiles > Web Application Firewall** and add or edit a Web Application Firewall profile and set **Inspection Device** to **External**.
5. Go to **Policy & Objects > IPv4 Policy**, add or edit a firewall policy, select **Web Application Firewall**, and select the profile that you set to use the external inspection device.

These steps add the following configuration to the CLI:

```
config system wccp
   set service-id 51
   set router-id 5.5.5.5 (the IP address of the FortiGate interface that communicates with
       the FortiWeb)
   set group address 0.0.0.0
   set server-list 5.5.5.25 255.255.255.255 (the IP address of the FortiWeb)
   set authentication enable
   set forward-method GRE
   set return-method GRE
   set assignment-method HASH
   set password *
end
```

Offloading HTTP traffic to FortiCache

To offload Web Caching to FortiCache a FortiGate must support WAN Optimization and WAN Optimization must be enabled. For some FortiGate models you need to turn off disk logging to support WAN Optimization. See "WAN Optimization" on page 203 in What's New for details.

Use the following steps to offload web caching to FortiCache. Using these steps you can select the web traffic to offload by selecting web caching in firewall policies. Only the web traffic accepted by those firewall policies will be offloaded.

A single FortiGate cannot offload HTTP traffic to both FortiCache and FortiWeb.

1. Go to the **System Information** dashboard widget and make sure **Inspection Mode** is set to **Proxy-based**.
2. Go to **System > Advanced > Disk Settings** and assign at least one disk to **WAN Optimization**.
3. Go to **System > Feature Select** and turn on **WAN Opt. & Cache**.
4. Go to **System > Cooperative Security Fabric**, enable **HTTP Service**, select **FortiCache** and add the IP addresses of your FortiCache devices. You can also select **Authentication** add a **password** if required.
5. Go to **Policy & Objects > IPv4 Policy**, add or edit a firewall policy and select **Web Cache**.

These steps add the following configuration to the CLI:

```
config system wccp
   set service-id 51
   set router-id 5.5.5.5 (the IP address of the FortiGate interface that communicates with
       the FortiCache)
   set group address 0.0.0.0
   set server-list 5.5.5.45 255.255.255.255 (the IP address of the FortiCache)
   set authentication enable
   set forward-method GRE
   set return-method GRE
   set assignment-method HASH
   set password *
end
```

Offloading SMTP traffic to FortiMail

Use the following steps to offload SMTP traffic to FortiMail to apply FortiMail features to the traffic. Using these steps you can select the SMTP traffic to offload by adding an AntiSpam profile configured for external inspection to selected firewall policies. Only the SMTP traffic accepted by those firewall policies is offloaded.

If you offload HTTP traffic to FortiWeb you can also apply other HTTP inspection to it from your FortiGate including virus scanning and web filtering.

To be able to offload Anti-Spam processing to a FortiMail device you should:

1. Go to the **System Information** dashboard widget and make sure **Inspection Mode** is set to **Proxy-based**.
2. Go to **System > Feature Select** and turn on **Anti-Spam Filter**.
3. Go to **System > Cooperative Security Fabric**, enable **SMTP Service - FortiMail** and add the IP address of your FortiMail devices. You can also select **Authentication** add a **password** if required.
4. Go to **Security Profiles > Anti-Spam** and edit an Anti-Spam profile and set **Inspection Device** to **External**.
5. Go to **Policy & Objects > IPv4 Policy**, add or edit a Firewall policy, enable **Anti-Spam** and select the profile for which you set Inspection Device to External.

These steps add the following configuration to the CLI:

```
config system wccp
   set service-id 52
   set router-id 5.5.5.5 (the IP address of the FortiGate interface that communicates with
       the FortiMail)
   set group address 0.0.0.0
   set server-list 5.5.5.65 255.255.255.255 (the IP address of the FortiMail)
   set authentication enable
   set forward-method GRE
   set return-method GRE
   set assignment-method HASH
   set password *
```

```
    end
```

Policy Learning Mode

Learning mode for Firewall policies (310544 365727)

The learning mode feature is a quick and easy method for setting a policy to allow everything but to log it all so that it can later be used to determine what restrictions and protections should be applied. The objective is to monitor the traffic not act upon it while in Learning mode.

Once the **Learn** action is enabled, functions produce hard coded profiles that will be enabled on the policy. The following profiles are set up:

- AntiVirus (`av-profile`)
- Web Filter (`webfilter-profile`)
- Anti Spam(`spamfilter-profile`)
- Data Leak Prevention (`dlp-sensor`)
- Intrusion Protection (`ips-sensor`)
- Application Control (`application-list`)
- Proxy Options (`profile-protocol-options`)

- These UTM profiles are all using Flow mode
- SSL inspection is always disable for the Learn option
- These profiles are static and cannot be edited.

Profiles that are not being used are:

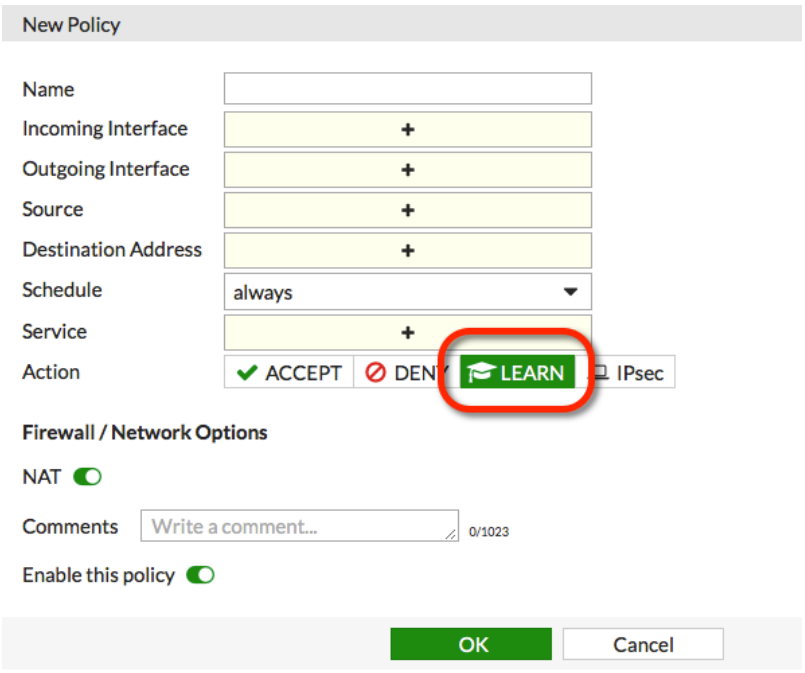
- DNS Filter (Does not have a Flow mode)
- Web Application Firewall(Does not have a Flow mode)
- CASI(Almost all signatures in CASI require SSL deep inspection. Without SSL inspection, turning on CASI serves little purpose)

The ability to allow policies to be set to a learning mode is enabled on a per VDOM basis.

```
config system settings
   set gui-policy-learning [enable | disable]
   end
```

Once the feature is enabled on the VDOM, Learn is an available **Action** option when editing a policy.

Because this feature requires a minimum level of logging capabilities, it is only available on FortiGates with hard drives. Smaller models may not be able to use this feature.



Once the Learning policy has been running for a sufficient time to collect needed information a report can be looked at by going to **Log & Report > Learning Report**.

The Report can be either a **Full Report** or a **Report Summary**

The time frame of the report can be **5 minutes**, **1 hour**, or **24 hours**.

The Learning Report includes:

Deployment Methodology

- Test Details
  - Start time
  - End time
  - Model
  - Firmware
- Policy List

Executive Summary

- Total Attacks Detected
- Top Application Category
- Top Web Category
- Top Web Domain
- Top Host by Bandwidth
- Host with Highest Session Count

Security and Threat Prevention

- High Risk Applications
- Application Vulnerability Exploits

- Malware, botnets and Spyware/Adware
- At-Risk Devices and Hosts

User Productivity

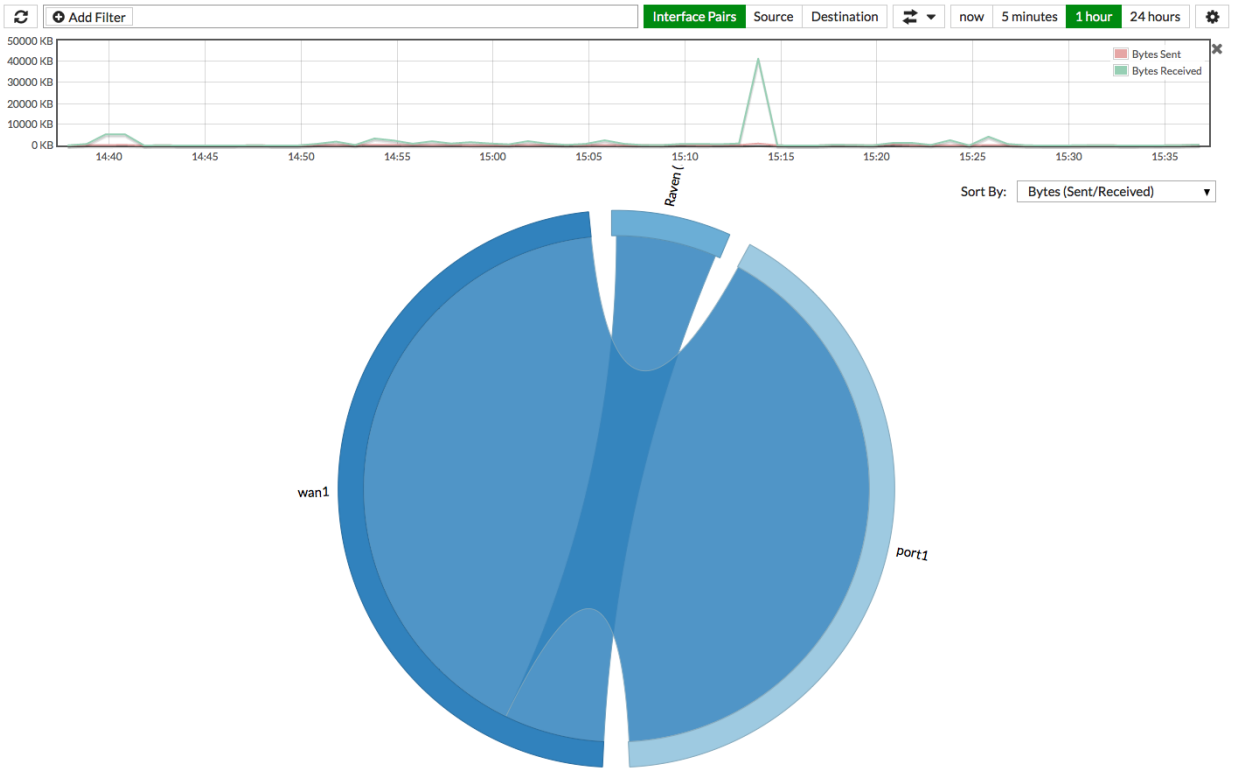
- Application Usage
  - Top Application Categories
  - Top Social Media Applications
  - Top Video/Audio Streaming Applications
  - Top Peer to Peer Applications
  - Top Gaming Applications
- Web Usage
  - Top Web Categories
  - Top Web Applications
  - Top Web Domains

FortiView

This chapter describes new FortiView features added to FortiOS 5.4.

New Interface Pair Visualization

A new visualization has been added to FortiView on the **Interfaces** page, with a cord chart showing which interfaces are connecting to each other, with comparative traffic volumes.



Notes about the Interface Pair Chart:

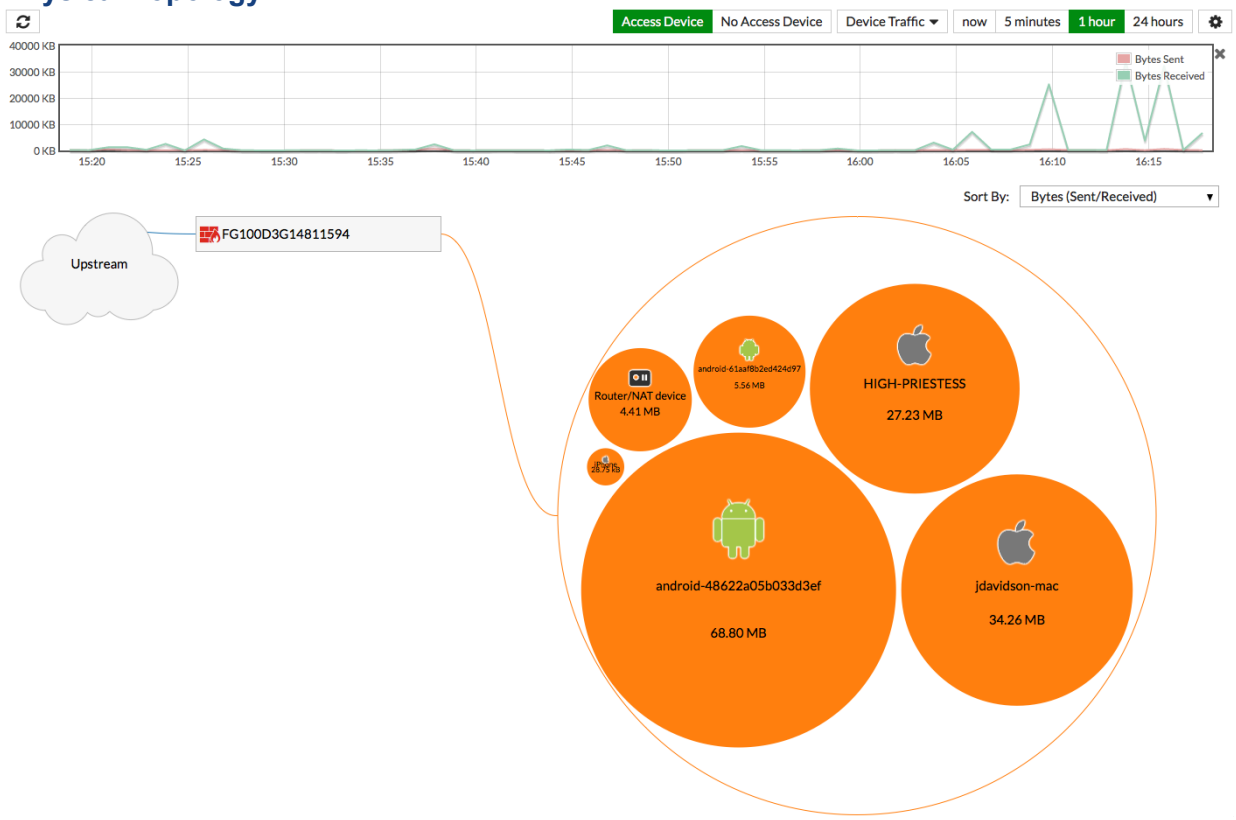
- It is possible to sort the Interface Pair Chart using the **Sort By:** dropdown menu.
- The width of each edge of the ring represents the volume of traffic.
- Place your cursor over an interface on the edge of the ring to hide all the other connections.
- You can mouse over the connecting cord to see a detail popup.

New Cooperative Security Fabric charts in FortiView (286116 308676)

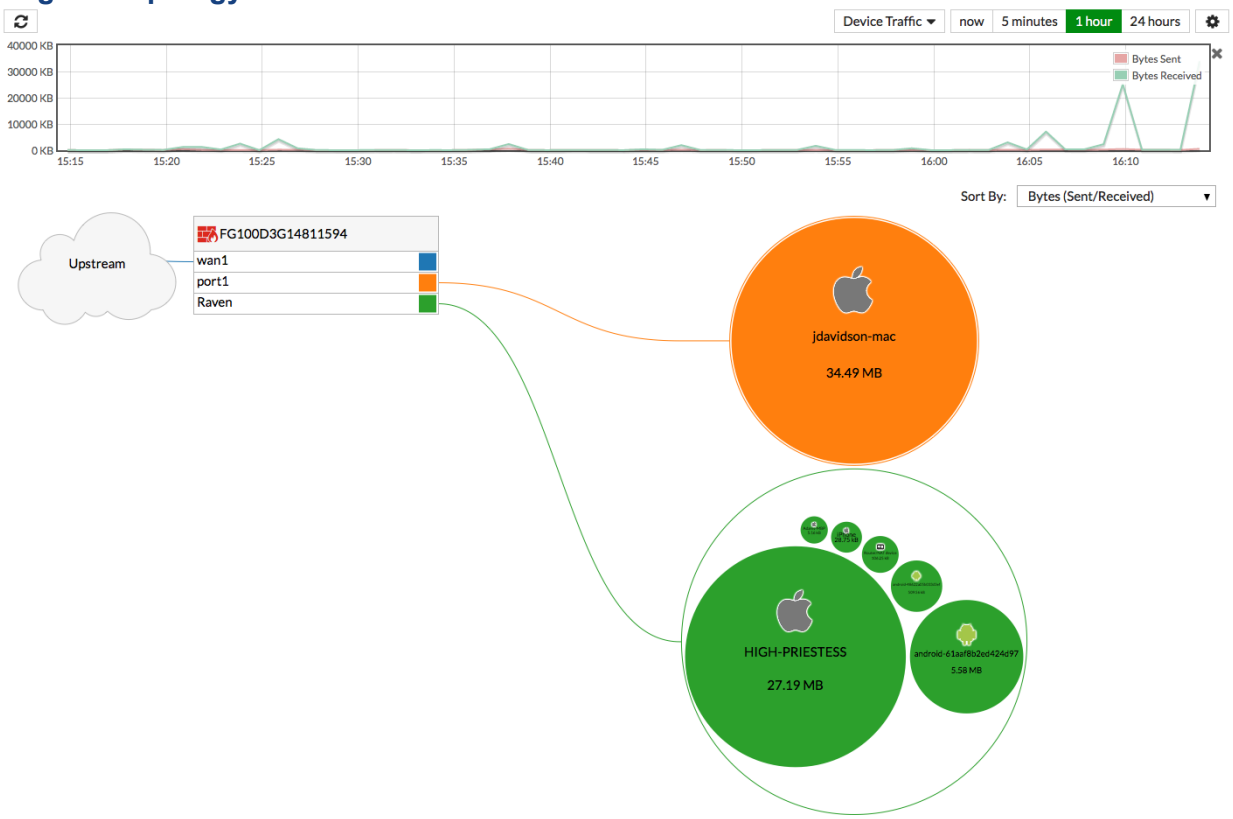
FortiOS 5.4.1 integrates the new Cooperative Security Fabric (CSF) features, which allow you greater control and oversight over your integrated network. For more on Cooperative Security Fabric, read the What's New section on CSF.

FortiView has integrated two new charts to support CSF in 5.4.1: **Physical Topology** and **Logical Topology**. They are scaled bubble charts that show the logical structure of your network, with upstream and downstream devices organized by connection.

Physical Topology



Logical Topology



Notes about the Topology Charts:

- It is possible to sort the Topology Charts using the **Sort By:** dropdown menu.
- You can customize what the bubble size represents with the dropdown next to the time selection.
- In Physical Topology, you can mouse over the bubbles and devices for overall device information.
- In Logical Topology, you can mouse over the bubbles and device ports for more detailed connection information.

FortiOS now supports more detailed geographic information (310567)

More granular city/town information has been added to the log system. It is not used in the management interface in 5.4.1, but is available in the CLI, with the command `diag geoip ip2country`.

New Search Phrases list available on the Web Sites page (303437)

FortiGate models 1500D and above now support 7-day view in FortiView (264331)

IPv6 policies appear in realtime FortiView displays (277558)

New Consoles

In FortiOS 5.4, a variety of new consoles have been added to FortiView:

FortiView Policies console

The new **Policies** console works similarly to other FortiView consoles, yet allows administrators to monitor policy activity, and thereby decide which policies are most and least active. This helps the administrator to discern which policies are unused and can be deleted.

In addition, you have the ability to click on any policy in the table to drill down to the Policies list and view or edit that policy. You can view this new console in either Table or Bubble Chart view.

FortiView Interfaces console

The new **Interfaces** console works similarly to other FortiView consoles and allows administrators to perform current and historical monitoring per interface, with the ability to monitor bandwidth in particular. You can view this new console in either Table or Bubble Chart view.

FortiView Countries console

A new **Countries** console has been introduced to allow administrators to filter traffic according to source and destination countries. This console includes the option to view the Country Map visualization (see below).

FortiView Device Topology console

The new **Device Topology** console provides an overview of your network structure in the form of a Network Segmentation Tree diagram (see below).

FortiView Traffic Shaping console

A new **Traffic Shaping** console has been introduced to improve monitoring of existing Traffic Shapers.

Information displayed includes Shaper info, Sessions, Bandwidth, Dropped Bytes, and more.

FortiView Threat Map console

A new **Threat Map** console has been introduced to monitor risks coming from various international locations arriving at a specific location, depicted by the location of a FortiGate on the map (see below).

FortiView Failed Authentication console

A **Failed Authentication** console has been added under **FortiView** that allows you to drill down an entry to view the logs. This new console is particularly useful in determining whether or not the FortiGate is under a brute force attack. If an administrator sees multiple failed login attempts from the same IP, they could (for example) add a local-in policy to block that IP.

The console provides a list of unauthorized connection events in the log, including the following:

- unauthorized access to an admin interface (telnet, ssh, http, https, etc.)
- failure to query for SNMP (v3) or outside of authorized range (v1, v2, v3)
- failed attempts to establish any of the following:
  - Dial-up IPsec VPN connections
  - Site-to-site IPsec VPN connections
  - SSL VPN connections
  - FGFM tunnel

FortiView WiFi Clients console

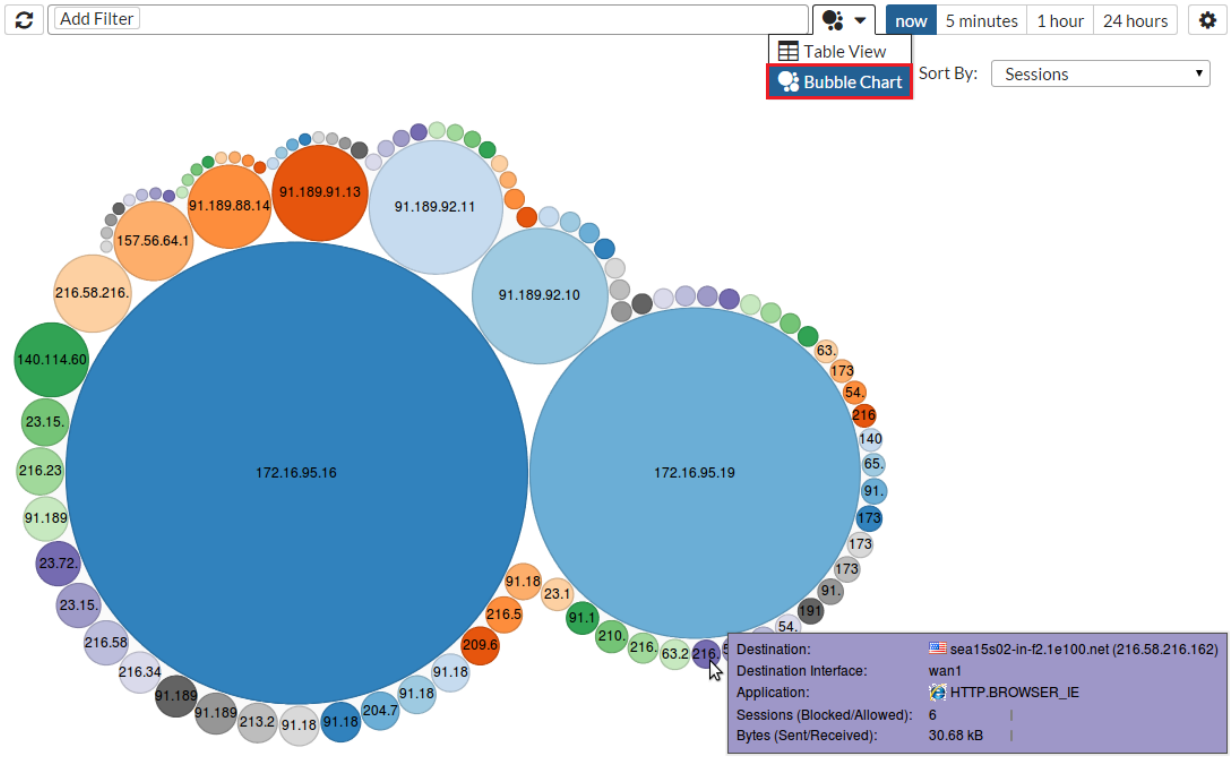
The WiFi Clients console has been added to FortiView in FortiOS 5.4. As you might expect, you can use this console to display top wireless user network usage and information. You can drilldown to filter the information that is displayed.

Information displayed includes Device, Source IP, Source SSID, AP, and more.

New FortiView Visualizations

New visualization support has been added to FortiView via the Bubble Chart and the Country Map.

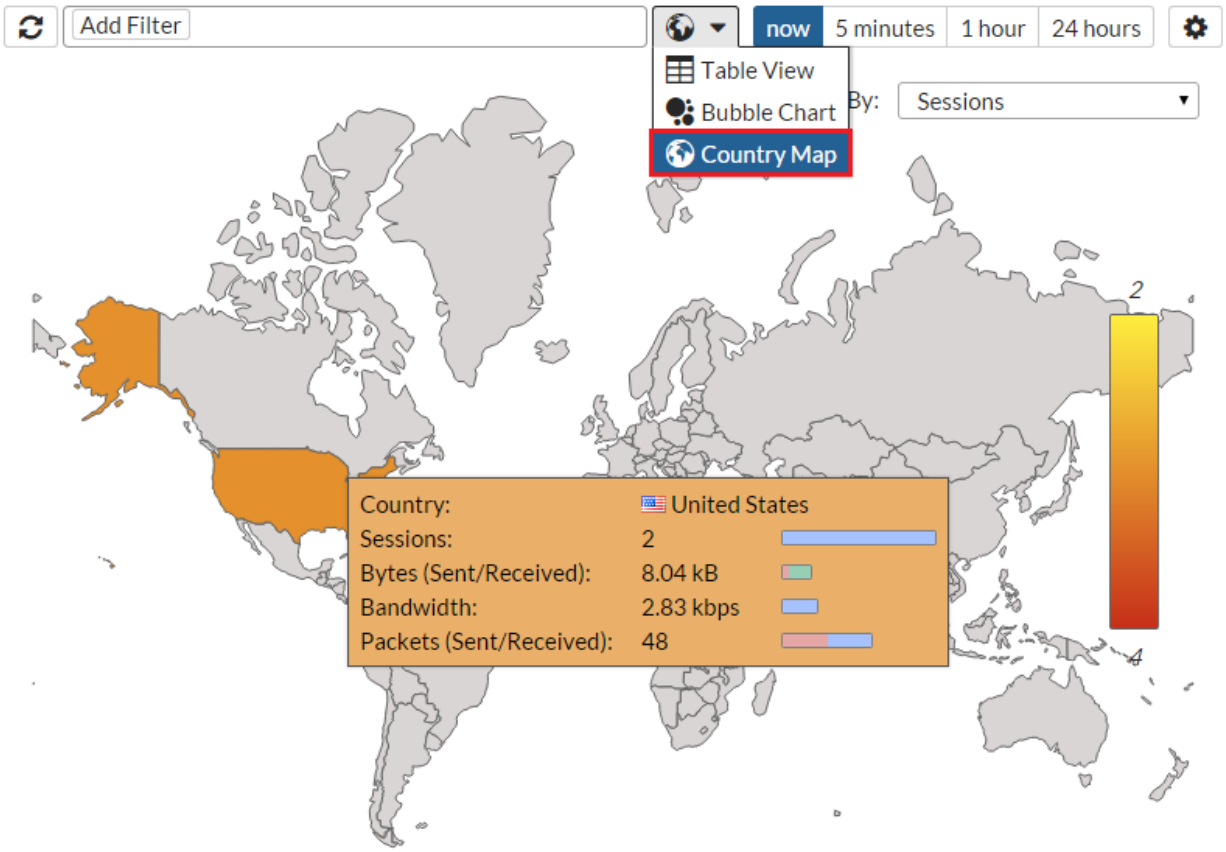
Bubble Chart Visualization



Notes about the Bubble Chart:

- It is possible to sort on the Bubble Chart using the **Sort By:** dropdown menu.
- The size of each bubble represents the related amount of data.
- Place your cursor over a bubble to display a tool-tip with detailed info on that item.
- You can click on a bubble to drilldown into greater (filtered) detail.

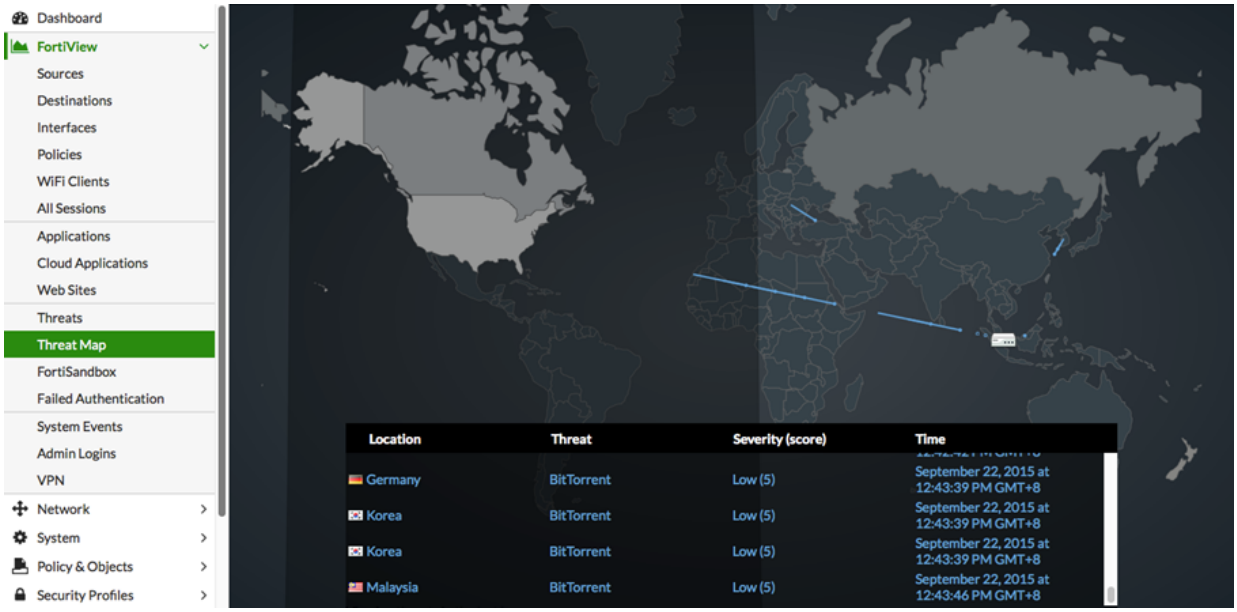
Country Map Visualization



Notes about the Country Map:

- The Country Map is only available in the Countries dashboard.
- It is possible to sort on the Country Map using the **Sort By:** dropdown menu.
- Place your cursor over any country to display a tool-tip with detailed info on that country's traffic.
- The colour gradiant on the map indicates the traffic load, where red indicates the more critical load.
- Click on any country to drilldown into greater (filtered) detail.

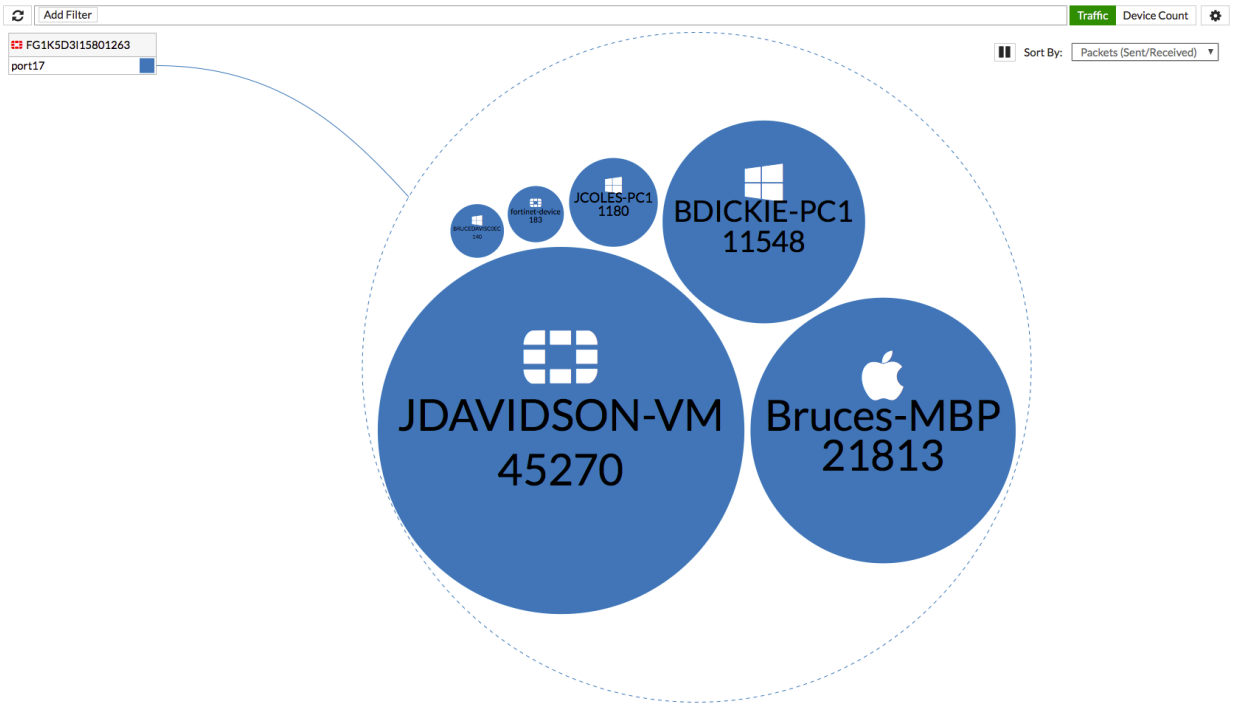
Threat Map Visualization



Notes about the Threat Map:

- Threats from various international destinations will be shown, but only those arriving at your destination, as depicted by the FortiGate.
- Place your cursor over the FortiGate's location to display the device name, the IP address, and the city name/location.
- A visual lists of threats is shown at the bottom, displaying the location, severity, and nature of the attacks.
- The colour gradiant of the darts on the map indicate the traffic risk, where red indicates the more critical risk.
- Click on any country to drilldown into greater (filtered) detail.

Device Topology Visualization



Notes about Device Topology:

- Place your cursor over any object in the visualization to display the device name, the IP address, Sessions, sent and received Bytes and Packets, Bandwidth, and Dropped Bytes.
- In many cases, such as Internal Network Firewall (INFW) deployments, there are multiple Fortigates performing NAT before a host reaches the external-facing WAN. In such a situation, a bubble chart depicting internal traffic may be inaccurate because the biggest bubble will be a Fortigate that is NAT'ing hundreds of endpoints behind it. This page solves that issue by ensuring all network elements are given visibility and structured in a human-readable format.

Realtime visualization

In addition to these new visualization options, you can now also enable realtime visualization.

To enable realtime visualization:

1. Click on the **Settings** icon next to the upper right-hand corner and select **Auto update realtime visualizations**. An option is displayed to set the **Interval (seconds)**. The maximum value is 300.
2. Enter a desired **Interval** and click **Apply**.

Links created between FortiView and View/Create Policy

The **Policy** column in FortiView consoles and the Log Viewer pages has changed to a link, which navigates to the IPv4 or IPv6 policy list and highlights the policy.

Right-clicking on a row in FortiView or the Log Viewer has menu items for **Block Source**, **Block Destination** and **Quarantine Source** where appropriate columns are available to determine these values. When multiple rows are selected, the user will be prompted to create a named **Address Group** to contain the new addresses.

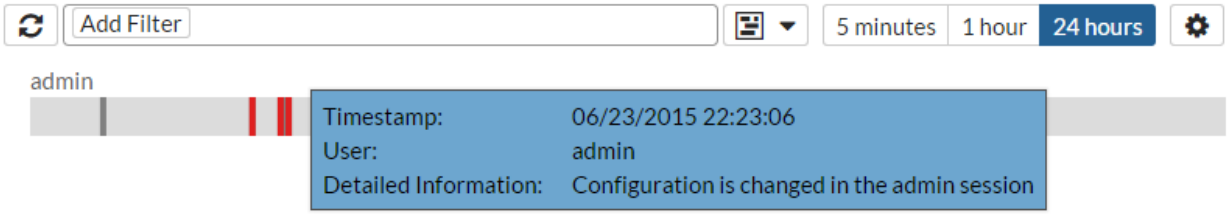
When the user clicks **Block Source** or **Block Destination** they are taken to a policy creation page with enough information filled in to create a policy blocking the requested IP traffic.

The policy page will feature an informational message block at the top describing the actions that will be taken. Once the user submits the form, the requisite addresses, groups and policy will be created at once.

If the user clicks on **Quarantine User** then they will be prompted for a duration. They may also check a box for a **Permanent Ban**. The user can manage quarantined users under **Monitor > User Quarantine Monitor**.

Visualization support for the Admin Logins page

A useful chart is now generated for Admin login events under **FortiView > Admin Logins**. You can view the information in either **Table View** or **Timeline View** (shown below). In Timeline View, each line represents on administrator, with individual sessions indicated per administrator line. When you hover over a particular timeline, detailed information appears in a tooltip.



New bandwidth column added to realtime FortiView pages

The FortiView console provides a new bandwidth column that displays information for bandwidth calculated on a per-session level, providing administrators the ability to sort realtime bandwidth usage in descending order.

Accelerated session filtering on All Sessions page

By default, on a FortiGate unit with NP6 processors, when you enable traffic logging in a firewall policy this also enables NP6 per-session accounting. If you disable traffic logging this also disables NP6 per-session accounting. This behavior can be changed using the following command:

```
config system np6
   edit np6_0
      set per-session-accounting {disable | all-enable | enable-by-log}
   end
```

By default, `per-session-accounting` is set to `enable-by-log`, which results in per-session accounting being turned on when you enable traffic logging in a policy. This configuration is set separately for each NP6 processor.

When offloaded sessions appear on the FortiView All Sessions console they include an icon identifying them as NP sessions:

Application	Bytes (Sent/Received)	Policy
TCP/443	29.16 kB	Local In
YouTube	NP 219.44 kB	my-policy
UDP/53	31.05 kB	Local In

You can hover over the NP icon to see some information about the offloaded sessions.

You can also use a FortiASIC Filter to view just the accelerated sessions.

WHOIS Lookup anchor for public IPv4 addresses

Reverse IP lookup is now possible in FortiOS 5.4. A WHOIS lookup icon is available when you mouse over a public IP address in a FortiView log. If you left-click on the lookup icon, a new tab is opened in your browser for www.networksolutions.com, and a lookup is performed on the selected IP address (this option persists after drilling down one level in FortiView).

FortiGuard Cloud App DB identification

FortiView now recognizes FortiGuard Cloud Application database traffic, which is mainly monitored and validated by FortiFlow, an internal application that identifies cloud applications based on IP, Port, and Protocol. Administrators can potentially use this information for WAN Link Load Balancing, for example.

7-day time display

In FortiOS 5.4, the following FortiGate models now support 7-day time display:

- FortiGate 1000D
- FortiGate 1500D
- FortiGate 3700DX
- FortiGate 3700D

The option for 7-day time display, however, can only be configured in the CLI using the following command:

```
config log setting
   set fortiview-weekly-data {enable|disable}
end
```

NP4 and NP6 icons showing accelerated sessions (282180)

When viewing sessions in the All Sessions console, information pertaining to NP4/ NP6 acceleration is now reflected via an appropriate icon. The tooltip for the icon includes the NP chip type and its total number of accelerated sessions.

Filtering on accelerated sessions (282180)

In addition to NP4/NP6 icons, you can now filter the console on 'FortiASIC' ('Accelerated' versus 'Not Accelerated') sessions.

WHOIS Lookup anchor for public IPv4 addresses (282701)

Reverse IP lookup is now possible in FortiOS 5.4. A WHOIS lookup icon is available when you mouse over a public IP address in a FortiView log. If you left-click on the lookup icon, a new tab is opened in your browser for www.networksolutions.com, and a lookup is performed on the selected IP address (this option persists after drilling down one level in FortiView).

New Report database construction (280398 267019)

This will improve performance with reports and FortiView without requiring any configuration changes.

Added a Timeline graph for admin events (271389)

Improved monitoring of traffic shapers; added traffic shaping to FortiView (290363)

Failed Authentication Attempts are now visible in FortiView (265890)

Added bandwidth column to FortiView (260896)

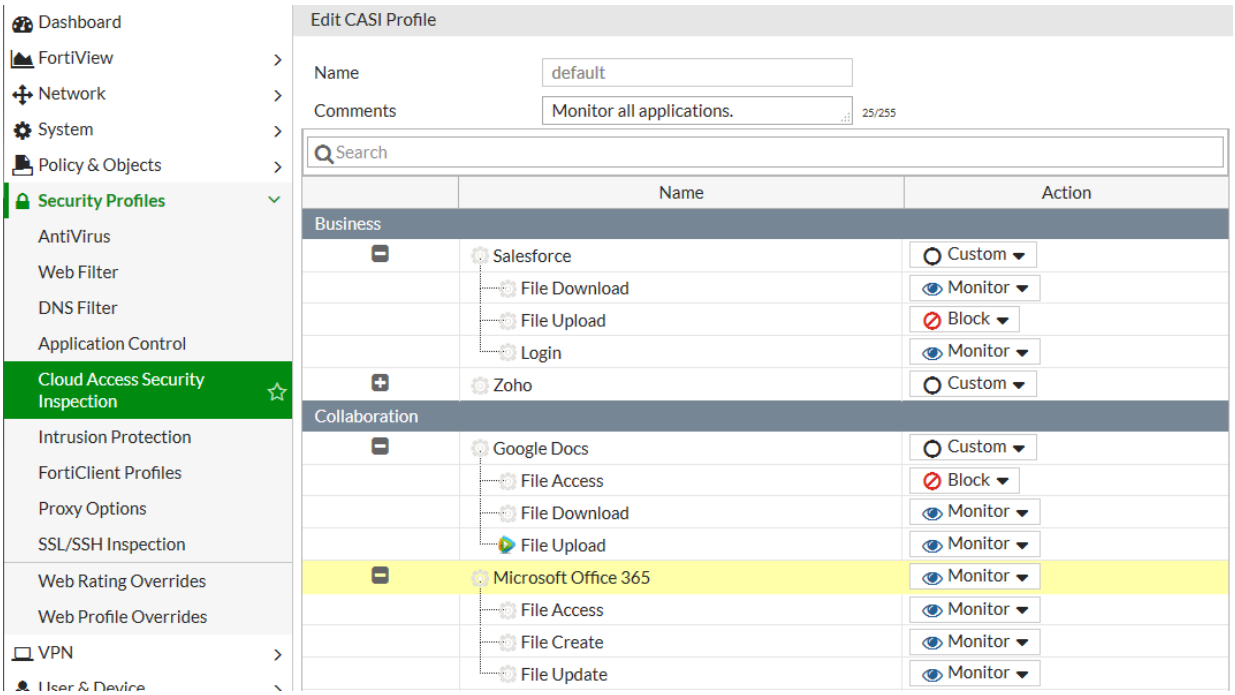
FortiView now displays Quarantine Source and appropriate icon in lists (289206)

Cloud Access Security Inspection (CASI)

Cloud Access Security Inspection (CASI)

This feature introduces a new security profile called Cloud Access Security Inspection (CASI) that provides support for fine-grained control on popular cloud applications, such as YouTube, Dropbox, Baidu, and Amazon. The CASI profile is applied to a policy much like any other security profile.

Unfortunately CASI does not work when using Proxy-based profiles for AV or Web filtering for example.
Make sure to only use Flow-based profiles in combination with CASI on a specific policy.



For this feature, **Deep Inspection of Cloud Applications** (`set deep-app-inspection [enable|disable]`) has been moved out of the **Application Control** security profile options.

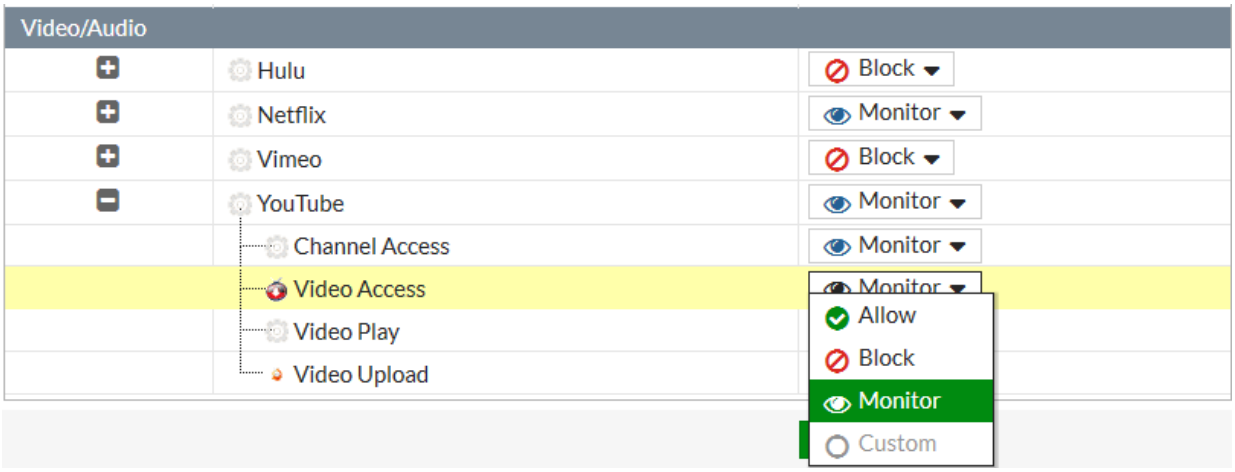
You will find the Cloud Access Security Inspection feature under **Security Profiles > Cloud Access Security Inspection**, but you must first enable it in the Feature store under **System > Feature Select > CASI**.

Editing CASI profiles

The CASI profile application list consists of the **Name**, **Category**, and **Action**. A default CASI profile exists, with the option to create custom profiles.

There is an **improvement to the CASI GUI (303760)** under release 5.4.1. When you search for a profile application to edit, you can hit enter after typing your search terms to see the results. Under release 5.4.0, hitting enter causes the screen to refresh and the profile to be applied.

For each CASI profile application, the user has the option to **Allow**, **Block**, or **Monitor** the selected cloud application. The following image demonstrates the ability to **Allow**, **Block**, or **Monitor** YouTube using CASI:



When the user drills down into a selected cloud application, the following options are available (depending on the type of service):

- **For business services, such as Salesforce and Zoho:** Option to allow, block, or monitor file download/upload and login.
- **For collaboration services, such as Google.Docs and Webex:** Option to allow, block, or monitor file access/download/upload and login.
- **For web email services, such as Gmail and Outlook:** Option to allow, block, or monitor attachment download/upload, chat, read/send message.
- **For general interest services, such as Amazon, Google, and Bing:** Option to allow, block, or monitor login, search phase, and file download/upload.
- **For social media services, such as Facebook, Twitter, and Instagram:** Option to allow, block, or monitor chat, file download/upload, post, login.
- **For storage backup services, such as Dropbox, iCloud, and Amazon Cloud Drive:** Option to allow, block, or monitor file access/download/upload and login.
- **For video/audio services, such as YouTube, Netflix, and Hulu**:
  Option to allow, block, or monitor channel access, video access/play/upload, and login.

CLI Syntax

```
configure application casi profile
   edit "profile name"
      set comment "comment"
      set replacemsg-group "xxxx"
      set app-replacemsg [enable|disable]
      configure entries
         edit
            set application "app name"
            set action [block|pass]
            set log [enable|disable]
         next
```

```
        edit 2
   next
end

configure firewall policy
   edit "1"
      set casi-profile "profile name"
   next
end

config firewall sniffer
   edit 1
      set casi-profile-status [enable|disable]
      set casi-profile "sniffer-profile"
   next
end

config firewall interface-policy
   edit 1
      set casi-profile-status [enable|disable]
      set casi-profile "2"
   next
end
```

Managed FortiSwitch

This chapter describes new managed FortiSwitch features added to FortiOS 5.4.

In FortiOS 5.4.2 and 5.4.1, all FortiGate models (except the FortiGate-80C) support managing FortiSwitches (FortiLink). Note that FortiSwitchOS 3.4.2 or later is required by all of the managed switches. See the FortiOS Feature/Platform matrix for more details and up-to-date compatibility info.

In FortiOS 5.4.0, the following FortiGate models support managed FortiSwitch:

FGT-60D, FGT-60D-POE, FWF-60D, FWF-60D-POE,
FGT-90D, FGT-90D-POE, FWF-90D, FWF-90D-POE,
FGT-100D, FGT-140D, FGT-140D_POE, FGT-140D_POE_T1,
FGT-200D, FGT-240D, FGT-280D, FGT-280D_POE,
FGT-600C, FGT-800C, FGT-1000C,
FGT-1200D, FGT-1500D, FGT-3700D

FortiLink is enabled by default on all physical FortiGate models. FortiLink is disabled by default on all of the FortiGate VMs.

FortiLink interface mode available for on all FortiGate models (309382)(279014)

In FortiOS 5.4.1, all FortiGate models (except the FortiGate-80C) support managing FortiSwitches (FortiLink). Note that FortiSwitchOS 3.4.2 or later is required by all of the managed switches. See the FortiOS Feature/Platform matrix for more details and up-to-date compatibility info.

FortiSwitch interface mode (305212) (279014) (294607)

With prior releases, the FortiGate required a separate FortiLink for each managed FortiSwitch. Starting in FortiOS 5.4.1, the FortiGate requires only one active FortiLink to manage all of the subtending FortiSwitches. The FortiSwitches are inter-connected and operate as one Layer 2 stack.

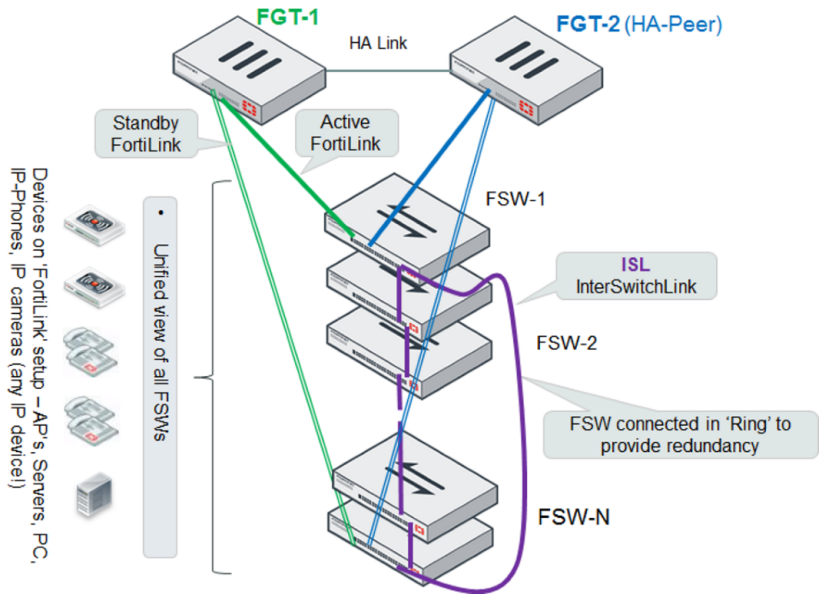
Depending on the network topology, you can also configure a standby FortiLink.

On the FortiGate, you configure the FortiLink as a single port or as a logical interface with multiple ports. The logical interface types supported include link-aggregation group (LAG), hardware switch and software switch.

FortiSwitch stacking (305212) (310481)

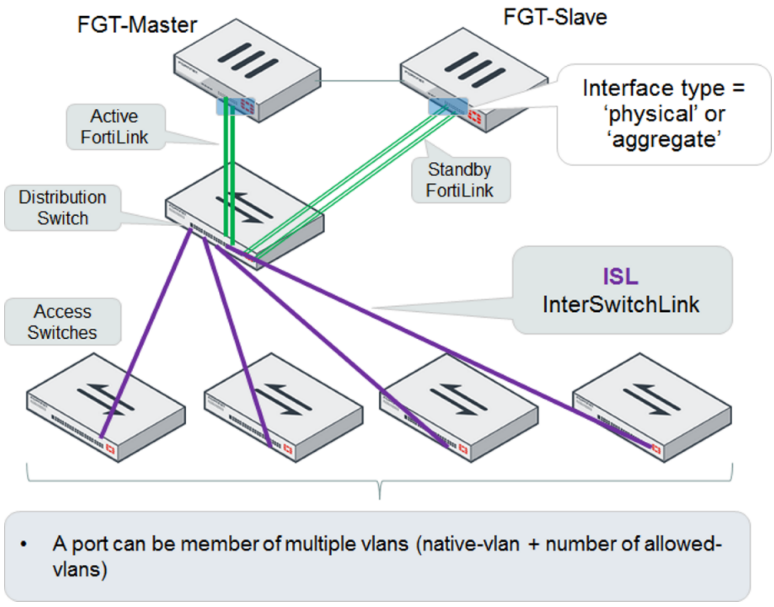
You can connect the managed FortiSwitches in a single-tier topology (aka Stack), or in a hierarchical topology.

In a single-tier topology, you connect a FortiLink from the FortiGate to one switch, and connect the switches in a ring using inter-switch links. Optionally, you can connect a standby FortiLink from the FortiGate to one of the other switches. This FortiLink remains in standby mode unless the active link fails. The following figure shows a single-tier topology with FortiGate HA:



In a hierarchical topology, the FortiSwitches are connected in two tiers, and operate as one Layer 2 cluster. You connect a FortiLink from the top-tier switch to the FortiGate, and the FortiGate then manages each switch separately.

Both topologies support FortiGate HA mode. The following figure shows a hierarchical topology with FortiGate HA:



Execute FortiSwitch commands from a FortiGate (300505)

From the FortiGate, you can execute FortiSwitch commands on the managed FortiSwitch.

This feature adds a simple scripting mechanism for users to configure generic commands to be executed on the switch.

Create a command

Use the following syntax to create a command file:

```
config switch-controller custom-command
   edit <cmd-name>
      set command " <FortiSwitch commands>"
```

The following example creates a command file to set the STP max-age parameter:

```
config switch-controller custom-command
   edit "stp-age-10"
      set command "config switch stp setting
         set max-age 10
         end
      "
   next
end
```

Execute a command

After you have created a command file, use the following command on the FortiGate to execute the command file on the target switch:

```
exec switch-controller custom-command <cmd-name> <target-switch>
```

The following example runs command **stp-age-10** on the specified target FortiSwitch:

```
FGT30E3U15003273 # exec switch-controller custom-command stp-age-10 S124DP3X15000118
```

Allow all defined VLANs in a FortiSwitch configuration (303818)

New port configuration option enables all defined vlans to be allowed on this port. The default value is disabled. This is a conveniece feature, to avoid having to configure all VLANs explicitly in the **allowed-vlans** field.

The following example shows the CLI commands to enable all VLANs on port1 of a managed switch:

```
FG080D3914002825 (managed-switch) # edit S124DN3W14000009
FG080D3914002825 (S124DN3W14000009) # config ports
FG080D3914002825 (ports) # edit port1
FG080D3914002825 (port1) # set allowed-vlans-all enable
```

When **allowed-vlans-all** is enabled, the **allowed-vlans** attribute is hidden.

FortiSwitch logs can be configured to be FortiOS system event logs (286258)

You can enable/disable the managed FortiSwitches to export their syslogs to the FortiGate. The setting is global, and the default setting is disabled.

The FortiGate sets the user field to "fortiswitch-syslog" for each entry, to allow a level of filtering.

CLI Command Syntax

```
config switch-controller switch-log
   status (enable | disable)
   severity [ emergency | alert | critical | error | warning | notification | information
       | debug ]
end
```

Stage or schedule FortiSwitch firmware upgrades (290916)

CLI Changes:

```
Stage FortiSwitch image to a managed FortiSwitch device.

execute switch-controller stage-swtp-image <vdom> <fortiswitch-id> <filename>
```

Example:

```
execute switch-controller stage-swtp-image root S124DN3W14000009 S124DN-IMG.swtp
S124DN3W14000009 # get system status
Version: FortiSwitch-124D v3.4.0,build0156,150929 (Interim)
S124DN3W14000009 # execute reboot
```

Display FortiSwitch port statistics in the FortiGate (303833)

Using the FortiGate CLI, display FortiSwitch port statistics.

Enter the following command. If you omit the port parameter, the FortiGate displays statistics for all of the ports:

```
diagnose switch-controller dump port-stats <switch id> <port>
```

The following example displays FortiSwitch port statistics for port1:

```
diagnose switch-controller dump port-stats S124DN3W14000095 port1
S124DN3W14000095 : Port1
tx-bytes 0, tx-packets 0, tx-mcast 0, tx-errors 0, tx-drops 0, tx-egoodpkts 0, rx-bytes 0,
    rx-packets 0,
rx-mcast 0, rx-errors 0, rx-drops 0, rx-emcasts 0, rx-ebroadcasts 0, rx-eundersize 0, rx-
    efragments 0, rx-eoversize 0, rx-ejabbers 0
rx-ecollisions 0, rx-ecrcalignments 0, rx-egoodpkts 0, rx-l3packets 0,
```

FortiLink per switch port connected device visibility (356560)(0357579) (302087) (303835) (357579)

In the FGT GUI, **User & Device** > **Device LIst** displays a list of devices attached to the FortiSwitch ports. For each device, table displays the IP address of the device, and the interface (FSW name and port).

From the CLI, the following command displays information about the host devices:

```
diagnose switch-controller dump mac-hosts_switch-ports
```

For each device, the CLI displays the IP address of the device, and the interface (FSW name and port).

Display FortiSwitches in Cooperative Security Fabric (CSF) Physical Topology (366873)

Each managed FortiSwitch is displayed as a device subtending the FortiGate.

Log message written when a FortiSwitch connects or disconnects (366519)

Add switch id to the log that is generated when a FortiSwitch connects to the FortiGate, or disconnects.

```
FS1D483Z14000057 is connected
FS1D483Z14000057 is disconnected
```

FortiGate CLI support for FortiSwitch features (on non-FortiLink ports)

You can configure additional FortiSwitch capabilities (STP, LAG, Storm Control) directly from the FortiGate, without the need to log in to the FortiSwitch.

Configuring STP

Starting in FortiSwitch release 3.4.2, STP is enabled by default for the non-FortiLink ports on the switch.

You can enable or disable STP globally, or per-switch-port.

Use the following CLI commands for global configuration:

```
config switch-controller stp-settings
   set status enable/disable
   set name <name>
   set revision <stp revision>
   set hello-time <hello time>
   set forward-time <forwarding delay>
   set max-age <maximum aging time>
   set max-hops <maximum number of hops>
end
```

Use the following commands for global configuration:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
         set stp-state (enabled | disabled)
end
```

Configuring LAG

You can configure a link aggregation group for non-fortilink ports on a FortiSwitch. You cannot configure ports from different FortiSwitches in one LAG.

```
config switch-controller managed-switch
   edit <switch-id>
```

```
      config ports
         edit <trunk name>
            set type trunk
            set mode < static | lacp > Link Aggreation mode
            set bundle (enable | disable)
            set min-bundle <int>
            set max-bundle <int>
            set members < port1 port2 ...>
         next
      end
   end
end
```

Configuring Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. Storm control uses the data rate of the link to measure traffic activity.

When the data rate exceeds the configured threshold, storm control drops excess traffic. You can configure the types of traffic to drop: broadcast, unknown unicast, or multicast.

The Storm Control settings are global to all of the non-FortiLink ports on the managed switches. Use the following CLI commands to configure storm control:

```
config switch-controller switch-storm-control
   set rate <rate>
   set unknown-unicast (enable | disable)
   set unknown-multicast (enable | disable)
   set broadcast (enable | disable)
end
```

The Rate units is packets per second. The default value is 500.

New FortiLink topology diagram (289005 271675 277441)

For managed FortiSwitches (**WIFI & Switch Controller > Managed FortiSwitch**), the system now displays the overall topology of the managed FortiSwitches that are connected to this FortiGate.

The topology lists the FortiLink ports on the FortiGate, and displays a full faceplate for each connected FortiSwitch (also showing the FortiLink ports on each FortiSwitch). You can right-click to authorize a managed FortiSwitch or left-click to edit the managed FortiSwitch information.

The topology can displays multiple FortiLinks to each FortiSwitch, as FortiOS 5.4 provides support for FortiLink as a LAG.

New interface option to auto-authorize extension devices 294966

If you enable the auto-authorize option on a FortiGate FortiLink port, the FortiGate will automatically authorize the managed FortiSwitch connected to this FortiLink. The new option is only visible when the interface type is set to **Dedicate to Extension Device**.

New CLI setting to enable pre-standard PoE detection on managed FortiSwitch ports 293512

This feature is available in FortiSwitchOS 3.3.2 and later releases.

Use the following commands to enable this setting on a managed FortiSwitch port:

```
config switch-controller managed-switch
   edit $FSW
      config ports
         edit "port1"
         set poe-pre-standard-detection enable/disable (the default is disable)
         next
      end
   end
```

Reset any POE port (by toggling the power OFF and then ON):

```
execute switch-controller poe-reset <fortiswitch-id> <port>
```

Display general POE status:

```
get switch-controller <fortiswitch-id> <port>
```

FortiGate HA cluster support for Managed Switches (276488)

Added the capability to support managed switches from a FortiGate HA cluster. If a standby FortiGate becomes active, it automatically establishes connectivity with the managed switches.

FortiLink GUI updates (288963)

New **VLAN** view to create and manage VLANs, including setting the VLAN id.

New **Ports** view of the managed FortiSwitches. The view now displays port status, including the assigned VLAN and the POE status for each port.

This view provides a clearer way to assign VLAN attributes to multiple ports on different FortiSwitches. The VLAN ID and color of each VLAN is clearly visible in the port assignment list. Also, when you configure a VLAN, you can now specify the VLAN ID.

Changing the FortiGate's inspection mode to flow or proxy

You can select Flow or Proxy Inspection Mode from the System Information dashboard widget to control your FortiGate's security profile inspection mode. Having control over flow and proxy mode is helpful if you want to be sure that only flow inspection mode is used (and that proxy inspection mode is not used).

Switching to Flow Inspection Mode also turns off WAN Optimization, Web Caching, the Explicit Web Proxy, and the Explicit FTP Proxy making sure that no proxying can occur.

In most cases proxy mode is preferred because more security profile features are available and more configuration options for these individual features are available. Some implementations; however, may require all security profile scanning to only use flow mode. In this case, you can set your FortiGate to flow mode knowing that proxy mode inspection will not be used.

If you select flow-based to use external servers for FortiWeb and FortiMail you must use the CLI to set a Web Application Firewall profile or Anti-Spam profile to external mode and add the Web Application Firewall profile or Anti-Spam profile to a firewall policy.

Changing between proxy and flow mode

Proxy mode is enabled by default and you change to flow mode by changing the **Inspection Mode** on the System Information dashboard widget.

When you select **Flow-based** you are reminded that all proxy mode profiles are converted to flow mode, removing any proxy settings. As well proxy-mode only features (for example, Web Application Profile) are removed from the GUI.

In addition, selecting **Flow-based** inspection will cause the **Explicit Web Proxy** and **Explicit FTP Proxy** features to be removed from the GUI and the CLI. This includes Explicit Proxy firewall policies.

When you select **Flow-based** you can only configure Virtual Servers (under **Policy & Objects > Virtual Servers**) with Type set to HTTP, TCP, UDP, or IP.

If required, you can change back to proxy mode through the System Information dashboard widget.

If your FortiGate has multiple VDOMs, you can set the inspection mode independently for each VDOM. Use the top left dropdown menu to go to **Global > System > VDOM**. Click **Edit** for the VDOM you wish to change and select the **Inspection Mode**.

Security profile features mapped to inspection mode

The table below lists FortiOS security profile features and shows whether they are available in flow-based or proxy-based inspection modes.

The DNS Filter security profile feature is only available for proxy-based inspection in FortiOS versions 5.4.0 and 5.4.1. It is available for both proxy-based and flow-based inspection in FortiOS versions 5.4.2 and above.

Security Profile Feature	Flow-based inspection	Proxy-based inspection
AntiVirus	x	x
Web Filter	x	x
DNS Filter	x	x
Application Control	x	x
Cloud Access Security Inspection	x	x
Intrusion Protection	x	x
Anti-Spam		x
Data Leak Protection		x
VoIP		x
ICAP		x
Web Application Firewall		x
FortiClient Profiles	x	x
Proxy Options		x
SSL/SSH Inspection	x	x
Web Rating Overrides	x	x
Web Profile Overrides		x

From the GUI, you can only configure antivirus and web filter security profiles in proxy mode. From the CLI you can configure flow-based antivirus profiles, web filter profiles and DLP profiles and they will appear on the GUI and include their inspection mode setting. Also, flow-based profiles created when in flow mode are still available when you switch to proxy mode.

In flow mode, antivirus and web filter profiles only include flow-mode features. Web filtering and virus scanning is still done with the same engines and to the same accuracy, but some inspection options are limited or not available in flow mode. Application control, intrusion protection, and FortiClient profiles are not affected when switching between flow and proxy mode.

CASI does not work when using proxy-based profiles for AV or Web filtering. Make sure to only use flow-based profiles in combination with CASI on a specific policy.

Even though VoIP profiles are not available from the GUI in flow mode, the FortiGate can process VoIP traffic. In this case the appropriate session helper is used (for example, the SIP session helper).

Setting flow or proxy mode doesn't change the settings available from the CLI. However, when in flow mode you can't save security profiles that are set to proxy mode.

You can also add proxy-only security profiles to firewall policies from the CLI. So, for example, you can add a VoIP profile to a security policy that accepts VoIP traffic. This practice isn't recommended because the setting will not be visible from the GUI.

Proxy mode and flow mode antivirus and web filter profile options

The following tables list the antivirus and web filter profile options available in proxy and flow modes.

Antivirus features in proxy and flow mode

Feature	Proxy	Flow
Scan Mode (Quick or Full)	no	yes
Detect viruses (Block or Monitor)	yes	yes
Inspected protocols	yes	no (all relevant protocols are inspected)
Inspection Options	yes	yes (not available for quick scan mode)
Treat Windows Executables in Email Attachments as Viruses	yes	yes
Send Files to FortiSandbox Appliance for Inspection	yes	yes
Use FortiSandbox Database	yes	yes
Include Mobile Malware Protection	yes	yes

Web Filter features in proxy and flow mode

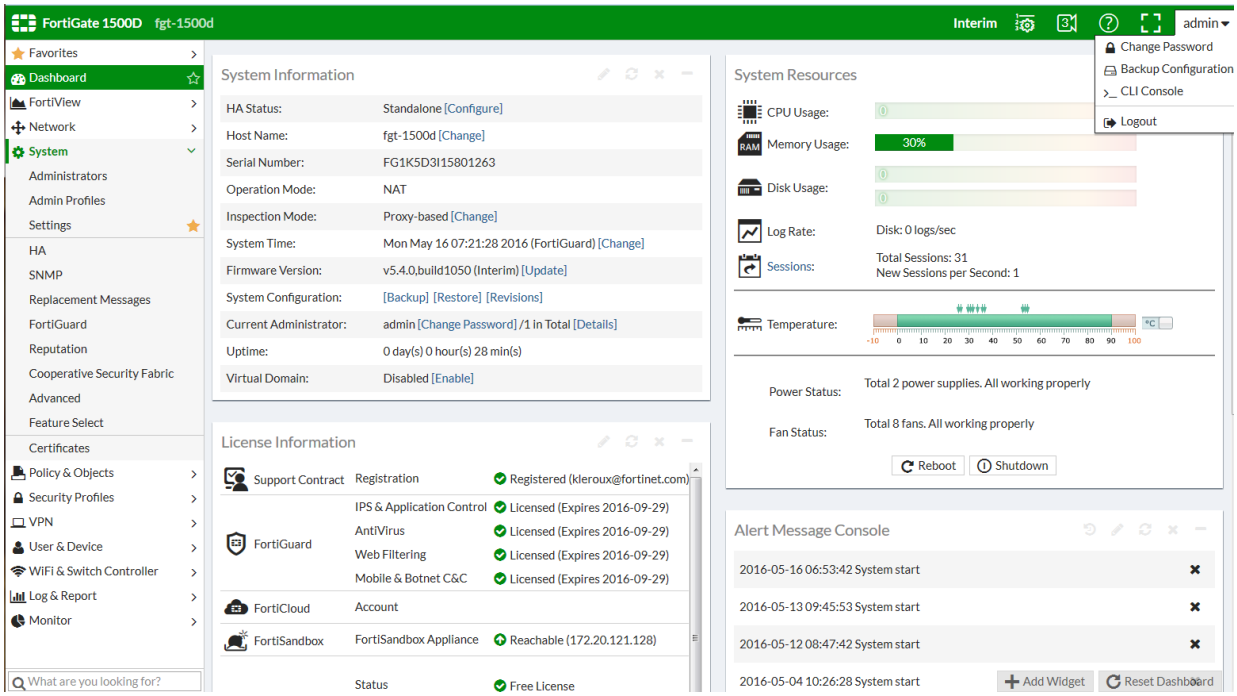
Feature	Proxy	Flow
FortiGuard category based filter	yes	yes (show, allow, monitor, block)
Category Usage Quota	yes	no
Allow users to override blocked categories (on some models)	yes	no
Search Engines	yes	no

Feature		Proxy	Flow
	Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	yes	no
	Restrict YouTube Access	yes	no
	Log all search keywords	yes	no
Static URL Filter		yes	yes
	Block invalid URLs	yes	no
	URL Filter	yes	yes
	Block malicious URLs discovered by FortiSandbox	yes	yes
	Web Content Filter	yes	yes
Rating Options		yes	yes
	Allow websites when a rating error occurs	yes	yes
	Rate URLs by domain and IP Address	yes	yes
	Block HTTP redirects by rating	yes	no
	Rate images by URL	yes	no
Proxy Options		yes	no
	Restrict Google account usage to specific domains	yes	no
	Provide details for blocked HTTP 4xx and 5xx errors	yes	no
	HTTP POST Action	yes	no
	Remove Java Applets	yes	no
	Remove ActiveX	yes	no
	Remove Cookies	yes	no
	Filter Per-User Black/White List	yes	no

GUI Refresh

The FortiGate GUI now uses a new flat GUI design and framework that incorporates a simplified and modern look and feel. In addition to the new look, options have been moved around on the GUI menus:

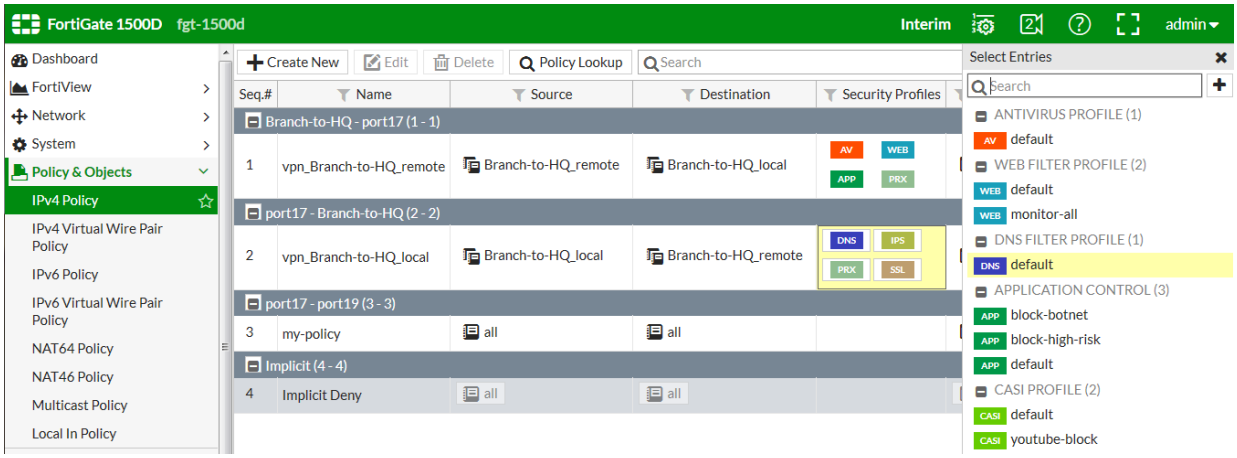
- New **Dashboard** and **FortiView** top level menus.
- New top level **Network** menu includes networking features such as interfaces, DNS, explicit proxy, packet capture, WAN links (WAN load balancing), static routing, policy routing, dynamic routing (RIP, OSPF, BGP) and multicast routing.
- New top level **Monitor** menu collects monitoring functions previously distributed throughout the GUI. Some former monitoring features, such as security profile-related monitoring, are now available in FortiView.
- The GUI menu now has two levels only. For example the menu path for accessing IPv4 firewall policies is **Policy & Objects > IPv4**.
- The new administrator's menu (upper right) provides quick access to change the administrator's password , backup the FortiGate configuration, access the CLI console and log out.
- Most individual GUI pages have also been enhanced with new view options and more information.
- Some functionality has moved around in the GUI. For example, **Proxy Options** and **SSL/SSH Inspection** moved from **Policy & Objects** to **Security Profiles**.



New options for editing policies from the policy list

All of the security policy lists (**Policy & Objects > IPv4** and so on) have new options for controlling the columns displayed for policies, for editing policies, and for accessing FortiView data or log messages generated by individual policies. You can access these options clicking or right-clicking on the policy list header or on individual policies.

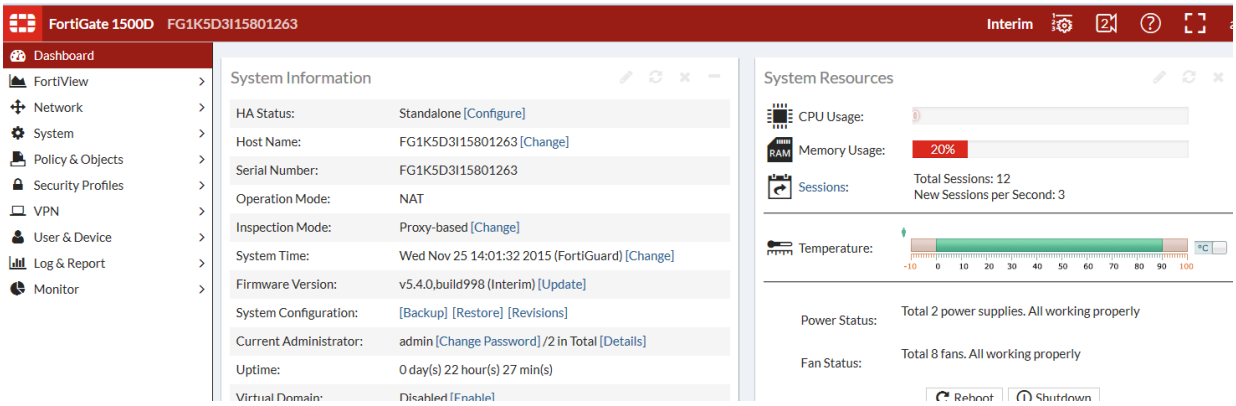
For example, as shown below if you click on the Security Profiles settings for a policy a list of categories and profiles appears on the left of the GUI. The list highlights the security profile options added to the policy. You can select a profile option to add it to a policy. You can deselect an option to remove it from a policy. Similar lists are available to select addresses, services, user groups, devices, and so on.



Changing the GUI theme

You can go to **System > Settings > View Settings** and select a **Theme**. You can also use the following CLI command to change the GUI theme. The following command shows how to change the GUI to use the red theme:

```
config system global
   set gui-theme red
end
```



Full screen mode

You can use the Full Screen Mode button (between the online help button and the admin menu) to toggle full screen mode. In full screen mode the GUI menu and header are hidden the full browser window is taken up by the current GUI page. You can select the Exit Full Screen mode any time to return to the normal GUI arrangement.

Edit in CLI

Available in the following locations among others in the FortiOS GUI you can select the Edit in CLI option to edit an item in the CLI.

- Firewall policy
- Firewall address
- Firewall service
- Firewall schedule
- Traffic shaper
- Shaping policy
- Policy route
- Static route
- Managed FortiAP

For example, if you are looking at a Firewall policy on the GUI and select Edit in CLI, the CLI console opens up inside the CLI configuration of the same policy. Some configurations options are only available from the CLI and this control allows you to easily edit specific items without having to find the item in the CLI.

Display the hostname on the GUI login page (129248)

- You can use the following CLI command to display the hostname on the GUI login page

```
config system global
   set gui-display-hostname {disable | enable}
end
```

Other GUI changes(129248)

- You can no longer add custom dashboard tabs. The following CLI command has been removed:

```
config system admin
   edit <admin>
      config dashboard-tabs
   end
```

- Lite version of the GUI (available on some low level models) has been removed including the following CLI command:

```
config system settings
   set gui-lite (disable | enable}
end
```

- You can no longer configure multiple custom dashboard widgets. The following CLI command has been removed:

```
config system admin
   edit <admin>
      config dashboard
         edit 0
            set widget-type app-usage
            set widget-type storage
            set widget-type protocol-usage
            set widget-type device-os-dist "Device/
         next
```

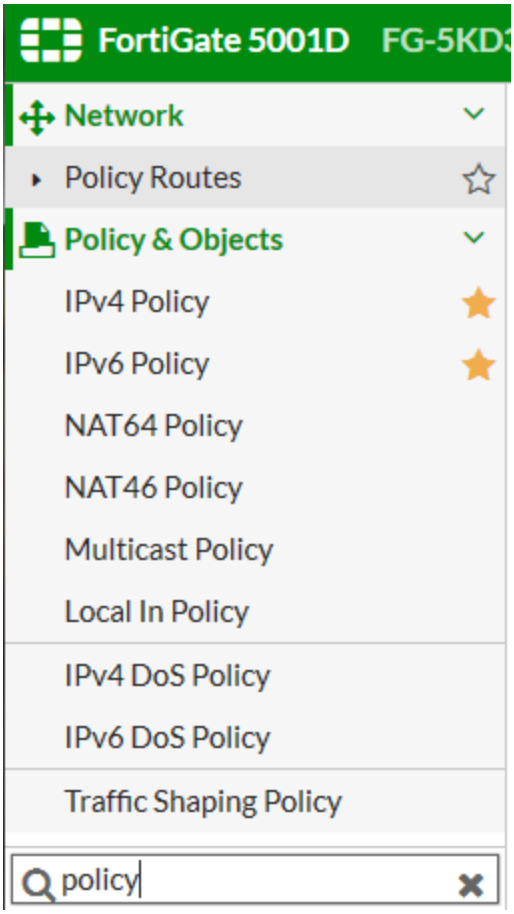
- HTTP obfuscating has also been removed, including the following CLI command.

```
config system global
   set http-obfuscate
end
```

GUI favorite and search (307478)

If there is a GUI page that you use often, rather than having to click through the GUI menu to find it you can select the star icon to make it a favorite page. Making something a favorite adds a new Favourites menu, which, when you open it, lists your favourite GUI pages. The GUI page at the top of the favourites list will be the page that appears the next time you log into the GUI. Favorites are saved for individual administrator accounts. Making a page a favourite doesn't remove it from its location in the GUI menu.

You can use the new search field at the bottom of the GUI menu to search for GUI page names. All of the GUI page names that match your appear and you can select the one you are looking for.



- Most diagnose sys dashboard commands removed (129248)

  The `diagnose sys dashboard reset` command is still available.

DNS Filter

Blocking DNS requests to known Botnet C&C addresses

A new FortiGuard database contains a list of known Botnet C&C addresses. This database is updated dynamically and stored on the FortiGate. This database is covered by FortiGuard web filter licensing, so you must have a FortiGuard web filtering license to use this feature.

When you block DNS requests to known Botnet C&C addresses, using IPS, DNS lookups are checked against the Botnet C&C database. All matching DNS lookups are blocked. Matching uses a reverse prefix match, so all sub-domains are also blocked.

To enable blocking of DNS requests to known Botnet C&C addresses, go to **Security Profiles > DNS Filter**, and enable **Block DNS requests to known botnet C&C**.

Static URL filter

The DNS inspection profile static URL filter allows you to block, exempt, or monitor DNS requests by using IPS to look inside DNS packets and match the domain being looked up with the domains on the static URL filter list. If there is a match the DNS request can be blocked, exempted, monitored, or allowed.

If blocked, the DNS request is blocked and so the user cannot look up the address and connect to the site.

If exempted, access to the site is allowed even if another method is used to block it.

DNS-based web filtering

This feature is similar to the FortiGuard DNS web filtering available in FortiOS 5.2. You can configure DNS web filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS web filtering is enabled, your FortiGate must use the FortiGuard DNS service for DNS lookups. DNS lookup requests sent to the FortiGuard DNS service return with an IP address and a domain rating that includes the FortiGuard category of the web page.

If that FortiGuard category is set to block, the result of the DNS lookup is not returned to the requester. If the category is set to redirect, then the address returned to the requester points at a FortiGuard redirect page.

You can also allow access or monitor access based on FortiGuard category.

CLI commands

Rename webfilter-sdns-server-ip and webfilter-sdns-server-port:

```
config system fortiguard
   set sdns-server-ip x.x.x.x
   set sdns-server-port 53
end
```

Configure DNS URL filter:

```
config dnsfilter urlfilter
   edit 1
```

```
      set name "url1"
      set comment ''
         config entries
            edit 1
               set url "www.google.com"
               set type simple
               set action block
               set status enable
            next
            edit 2
               set url "www.yahoo.com"
               set type simple
               set action monitor
               set status enable
            next
            edit 3
               set url "www.foritnet.com"
               set type simple
               set action allow
               set status enable
            next
         end
   next
end
```

Configure DNS filter profile:

```
config dnsfilter profile
   edit "dns_profile1"
      set comment ''
         config urlfilter
            set urlfilter-table 1
         end
         config ftgd-dns
               config filters
                  edit 1
                     set category 49
                     set action block
                     set log enable
                  next
                  edit 2
                     set category 71
                     set action monitor
                     set log enable
                  next
               end
         end
      set log-all-url disable
      set block-action redirect
      set redirect-portal 0.0.0.0
      set block-botnet enable
   next
end
```

Configure DNS profile in a firewall policy:

```
config firewall policy
   edit 1
```

```
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "FTP"
        set utm-status enable
        set dnsfilter-profile "dns_profile1"
        set profile-protocol-options "default"
        set nat enable
    next
end
```

Configure DNS profile in profile group:

```
config firewall profile-group
    edit "pgrp1"
        set dnsfilter-profile "dns_profile1"
        set profile-protocol-options "default"
    next
end
```

FortiSandbox Integration

This chapter describes new FortiSandbox features added to FortiOS 5.4.

FortiSandbox Log entry (302818)

Users can correlate submissions to FortiSandbox with the verdict on those files by viewing results at **Log & Report > AntiVirus**.

Changes to FortiSandbox inspection options in AntiVirus profile

When configuring the AntiVirus profile's inspection options, users can withhold files from being submitted for inspection by type or by name pattern.

Changes to FortiSandbox GUI configuration options (354523)

This change allows you to enable the FortiSandbox appliance from the Dashboard's License Information widget.

1. Go to **Dashboard**. Locate the License Information widget and click on the **Configure** button in the FortiSandbox row.
2. You will be directed to the **System > Cooperative Security Fabric** page.

NOTE: Continue with steps 3 to 9 under **Connecting to a FortiSandbox** below.

FortiSandbox Integration with FortiOS

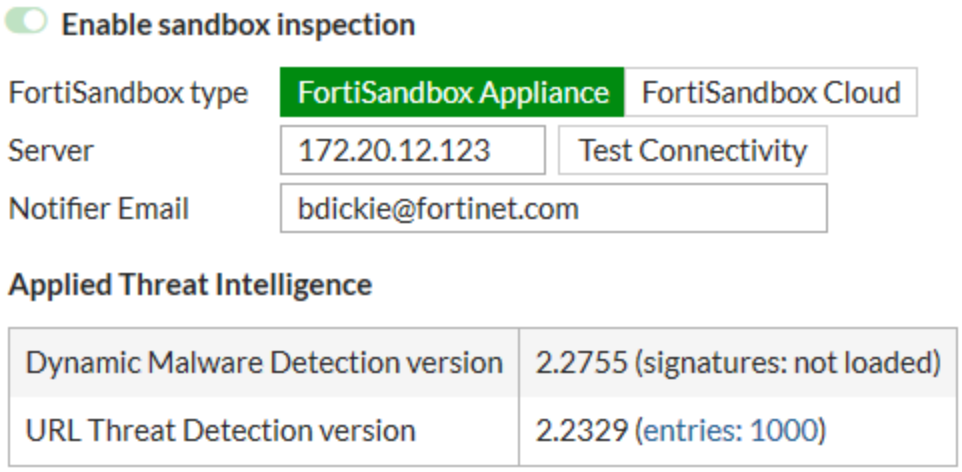
The following improvements have been made to how sandboxing, using either a FortiSandbox Appliance or FortiCloud Sandboxing, integrates with a FortiGate unit.

See the Cookbook recipe Sandboxing with FortiSandbox and FortiClient, http://cookbook.fortinet.com/sandboxing-fortisandbox-forticlient-54/.

Connecting to a FortiSandbox

1. Go to **System > Cooperative Security Fabric** and select **Enable Sandbox Inspection**.
2. You can either select **FortiSandbox Appliance** or **FortiSandbox Cloud**.

3. If you select FortiSandbox Appliance, add the **Server** IP address.

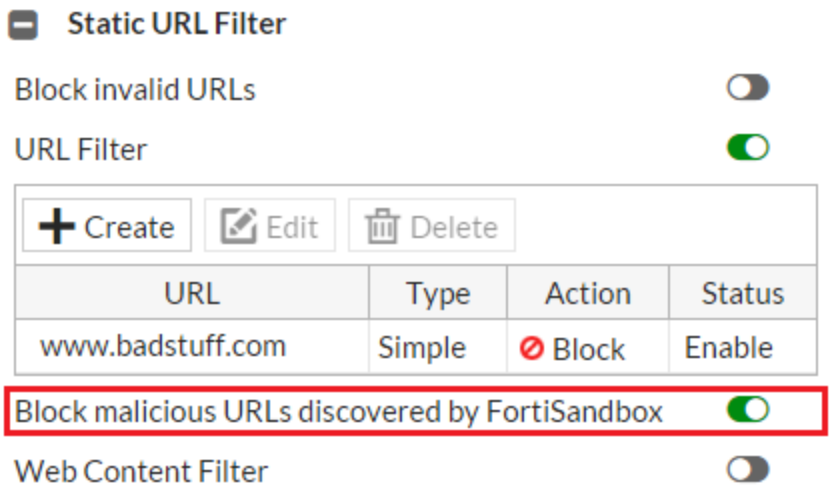


4. Select **Test Connectivity** to verify that you can connect to FortiSandbox.
5. Then edit an AntiVirus profile by going to **Security Profiles > AntiVirus** and selecting **Send Filter to FortiSandbox Appliance for Inspection**.
6. In FortiOS 5.4.0, you can also elect to send Suspicious Files, Executable files or all supported files.
   In FortiOS 5.4.1, you can choose to **Treat Windows Executables in Email Attachments as Viruses** and **Send All Supported Files**. When you select **Send All Supported Files**, you then have the option of withholding files from FortiSandbox inspection by type or by name pattern.
7. Select **Use FortiSandbox Database** to add signatures for suspicious files found by FortiSandbox to your FortiGate antivirus signature database.
8. Then add this AntiVirus profile to a firewall policy to send files in traffic accepted by the firewall policy to FortiSandbox.
9. You can also go to **Security Profiles > Web Filter** and select **Block malicious URLs discovered by FortiSandbox**.

Pushing malicious URLs to Web Filtering

The malicious URL database contains all malicious URLs active in the last month. The FortiSandbox can add the URLs where any malicious files originated to a URL filter, to block these files from being downloaded again from that URL.

This feature is enabled in a Web Filter profile under **Security Profiles > Web Filter > Block malicious URLs discovered by FortiSandbox**.



CLI Syntax

```
config webfilter profile
   edit <profile>
      config web
         ...
         set blacklist [enable | disable]
         ...
      end
```

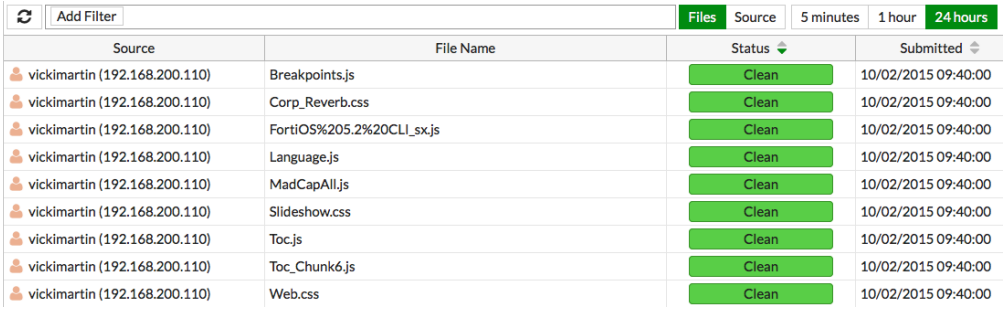
Files blocked by a FortiSandbox signature can be viewed and filtered for in the FortiSandbox dashboard. Information on the current database for both malware signatures and blocked URLs can be found by going to **System > Cooperative Security Fabric**.

FortiSandbox statistics (last 7 days)

File type	Detected
Total submitted	0
Malicious	0
Suspicious (high risk)	0
Suspicious (medium risk)	0
Suspicious (low risk)	0
Clean	0

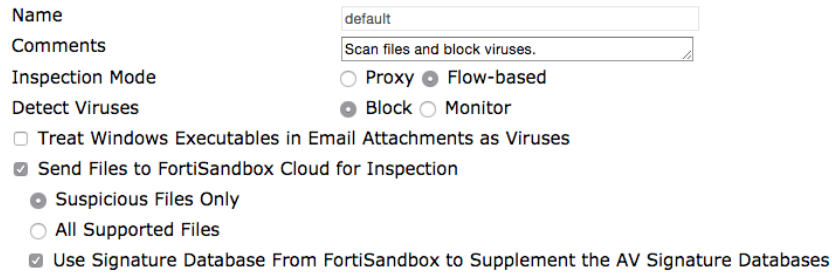
FortiSandbox Dashboard in FortiView

The FortiSandbox dashboard is available from **FortiView > FortiSandbox**. The dashboard shows all samples submitted for sandboxing. Information on the dashboard can be filtered by checksum, file name, result, source, status, and user name. Each entry also offers a drilldown view to show more details about a particular sample.



Pushing signatures to AntiVirus database

When a FortiSandbox discovers a malicious file, it can create a signature that is sent to the FortiGate to supplement the AntiVirus signature database. This signature can be used to block that file from entering the network again, and to prevent duplicates of the file being sent to the FortiSandbox in the future. This feature is enabled in an AntiVirus profile.



CLI Syntax

```
config antivirus profile
   edit "default"
      set ftgd-analytics {everything | suspicious}
      set analytics-db {enable | disable}
   end
```

Files blocked by a FortiSandbox signature can be viewed in entirety or as a filtered list in the FortiSandbox dashboard.

Information on the current database for malware signatures and blocked URLs can be found by going to **System > Cooperative Security Fabric**.

FortiSandbox statistics (last 7 days)

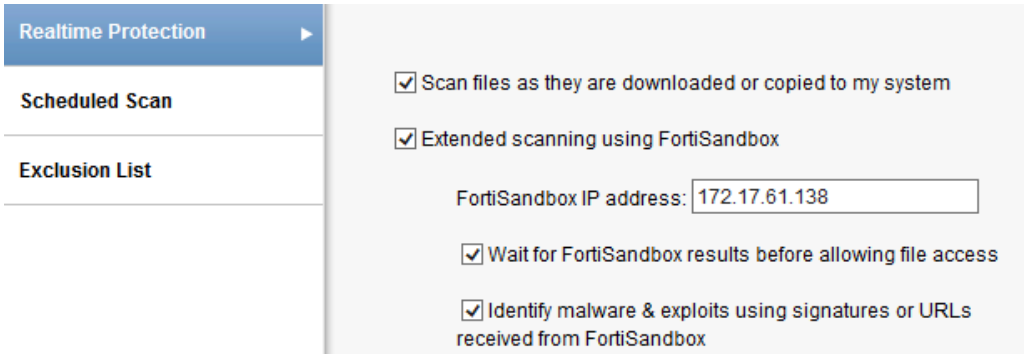
File type	Detected
Total submitted	0
Malicious	0
Suspicious (high risk)	0
Suspicious (medium risk)	0
Suspicious (low risk)	0
Clean	0

FortiClient Monitoring and Quarantine

FortiClient monitoring and quarantine is currently only supported by FortiClient 5.4 for Windows.

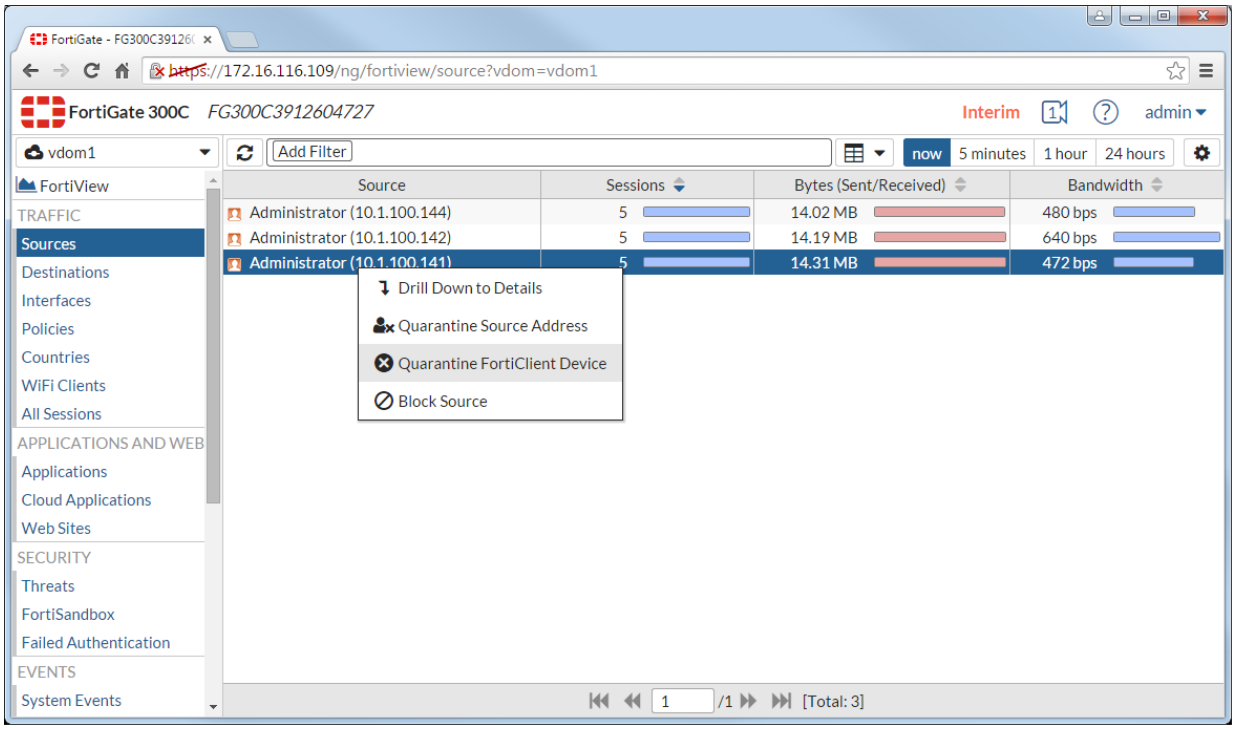
FortiSandbox uses a single signature to identify tens of thousands of variations of viral code. A FortiSandbox can send frequent, dynamic signature updates to a FortiGate and FortiClient, which allows files to be blocked before they are sent to the FortiSandbox.

With FortiSandbox, FortiClient, and FortiGate integration, you can configure a FortiGate to send files to FortiSandbox for scanning.

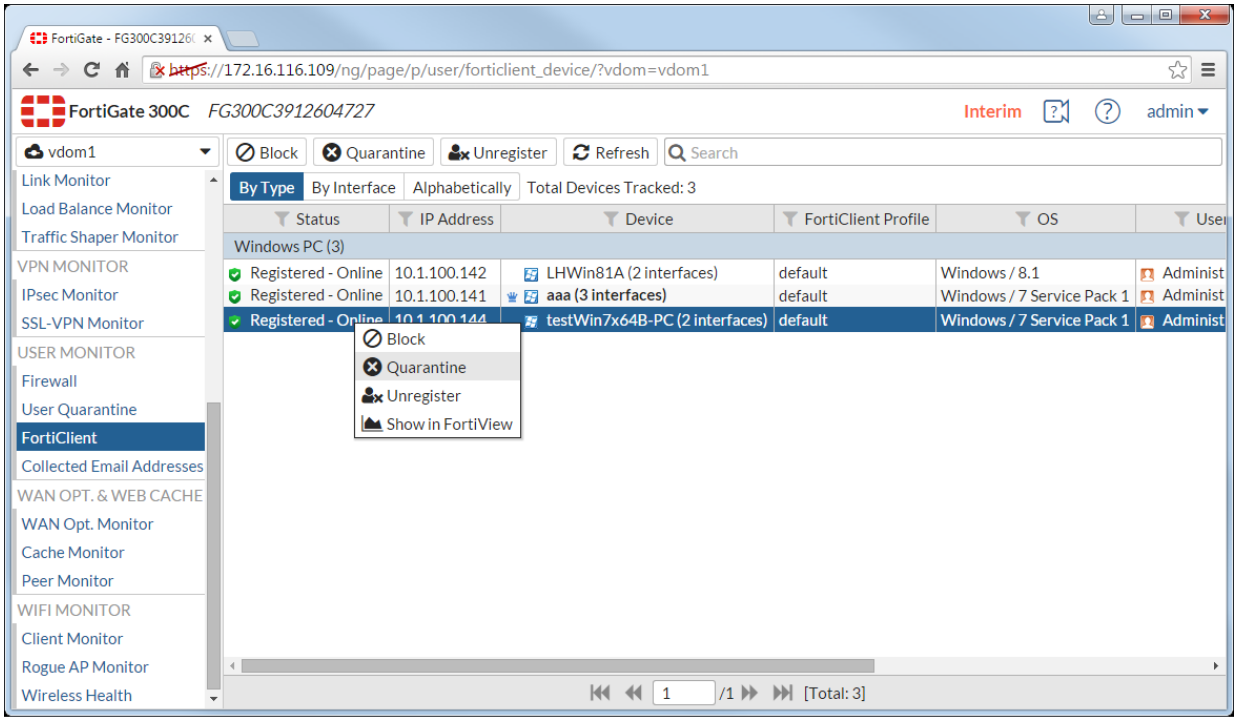


When FortiSandbox determines that a file is infected, it will notify the FortiGate of this event. Then, from FortiView, the administrator can take action to quarantine the endpoint which downloaded the infected file.

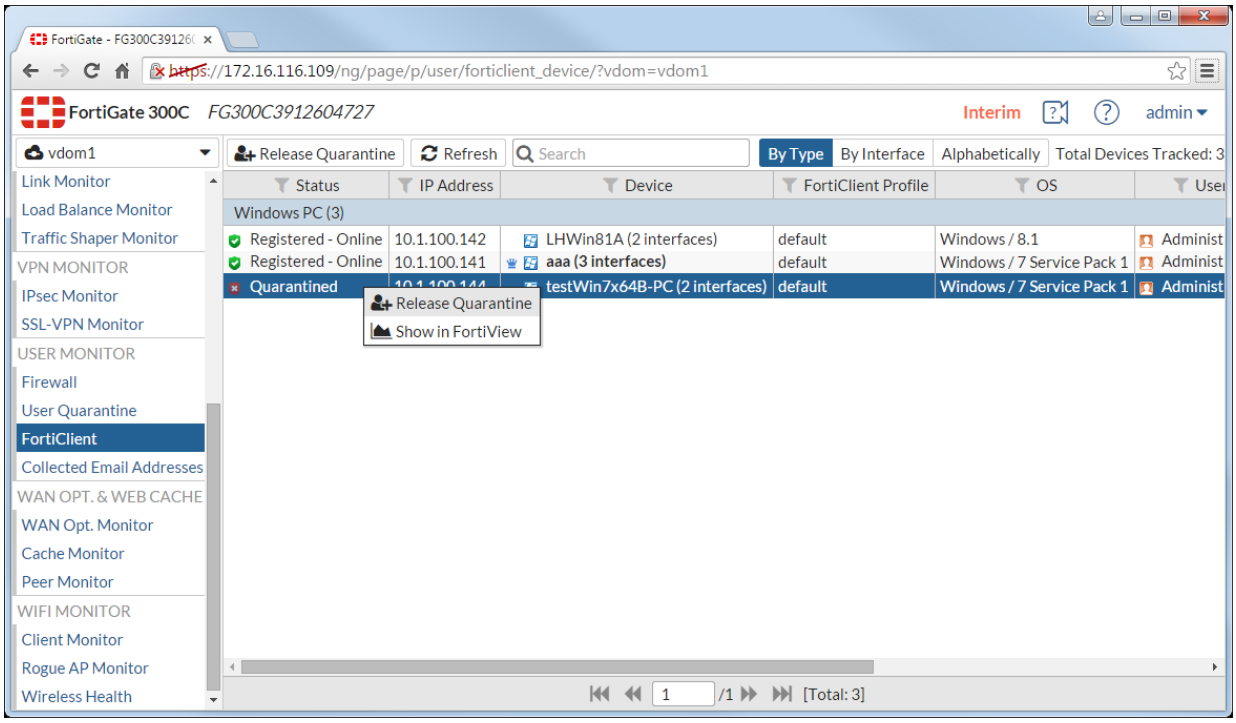
FortiGate administrators can quarantine endpoints from FortiView.



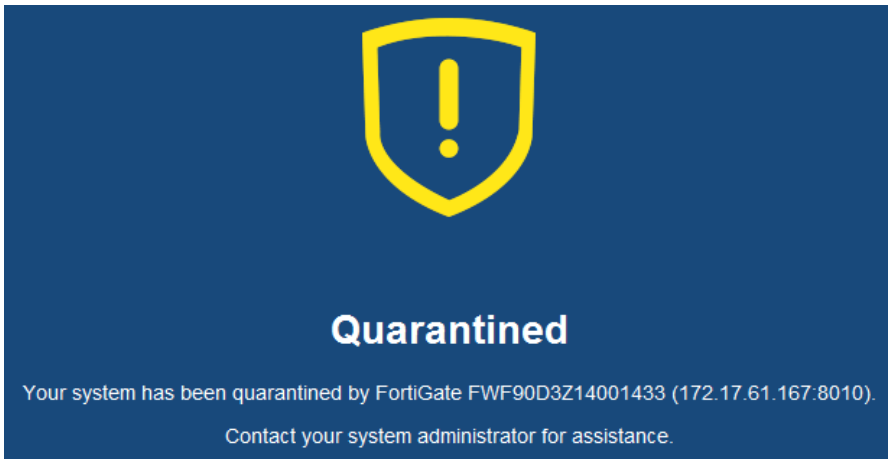
FortiGate administrators can also quarantine endpoints from the FortiClient Monitor.



FortiGate administrators can also manually release a quarantined endpoint.



To support this, the FortiClient now supports host-level quarantine by cuting off other network traffic from the endpoint directly and preventing it from infecting or scanning the local network.



When a device is under quarantine, FortiClient cannot be shutdown or uninstalled. A user is also unable to unregister from the FortiGate that quarantined them, or register to another FortiGate unit.

Alternately, FortiGate can release the file to the client before receiving the FortiSandbox scan results, and then have FortiClient quarantine the device when the scan results are available if required.

Traffic Shaping Policies

This chapter describes new traffic shaping features added to FortiOS 5.4.

Traffic shaping policy IDs added to traffic logs (303802)

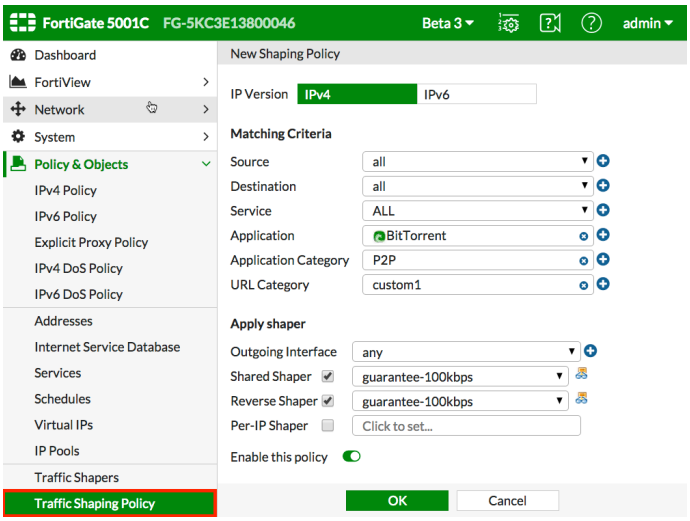
As of build 1013, traffic shaping policy IDs are now displayed in traffic logs and IP sessions. This allows you to easily identify which shaping policy is applied to traffic, even with multiple shaping policies configured. Look at the example below to see a sample log with the `shapingpolicyid`:

```
date=2016-01-29 time=15:35:25 logid=0000000013 type=traffic subtype=forward
level=notice vd=vdom1 srcip=192.0.2.2 srcname="A" srcport=43041
srcintf="port3" dstip=203.0.113.55 dstport=80 dstintf="port11"
poluuid=bcd3b008-c6bd-51e5-0e2c-2002e7a5774d sessionid=18364 proto=6
action=close policyid=2 policytype=policy dstcountry="Reserved"
srccountry="Reserved" trandisp=snat transip=192.0.2.2 transport=43041
service="HTTP" duration=205 sentbyte=747285 rcvdbyte=26382426 sentpkt=12887
rcvdpkt=17592 shapingpolicyid=1 shapersentname="shaper400"
shaperdropsentbyte=0 shaperrcvdname="shaper200" shaperdroprcvdbyte=14065762
appcat="unscanned" devtype="Fortinet Device" osname="Fortinet OS"
mastersrcmac=33:5b:0e:ca:dd:dc srcmac=33:5b:0e:ca:dd:dc
```

New Traffic Shaper Policy Configuration Method (269943)

Previously, traffic shapers were configured in **Policy & Objects > Objects > Traffic Shapers** and then applied in security policies under **Policy & Objects > Policy > IPv4** . In FortiOS 5.4, traffic shapers are now configured in a new traffic shaping section in **Policy & Objects > Traffic Shapers**.

The way that traffic shapers are applied to policies has changed significantly in 5.4., because there is now a specific section for traffic shaping policies in **Policy & Objects > Traffic Shaping Policy**. In the new traffic shaping policies, you must ensure that the **Matching Criteria** is the **same** as the security policy or policies you want to apply shaping to. The screen shot below shows the new 5.4 GUI interface:



There is also added Traffic Shaper support based on the following:

- Source (Address, Local Users, Groups)
- Destination (Address, FQDN, URL or category)
- Service (General, Web Access, File Access, Email and Network services, Authentication, Remote Access, Tunneling, VoIP, Messaging and other Applications, Web Proxy)
- Application
- Application Category
- URL Category

Creating Application Control Shapers

Application Control Shapers were previously configured in the **Security Profiles > Application Control** section, but for simplicity they are now consolidated in the same section as the other two types of traffic shapers: Shared and Per-IP.

To create an Application Control Shaper, you must first enable application control at the policy level, in **Policy & Objects > Policy > [IPv4 or IPv6]**. Then, you can create a matching application-based traffic shaping policy that will apply to it, in the new Traffic Shaping section under **Policy & Objects > Traffic Shaping Policy**.

New attributes added to "firewall shaping-policy" (277030) (275431)

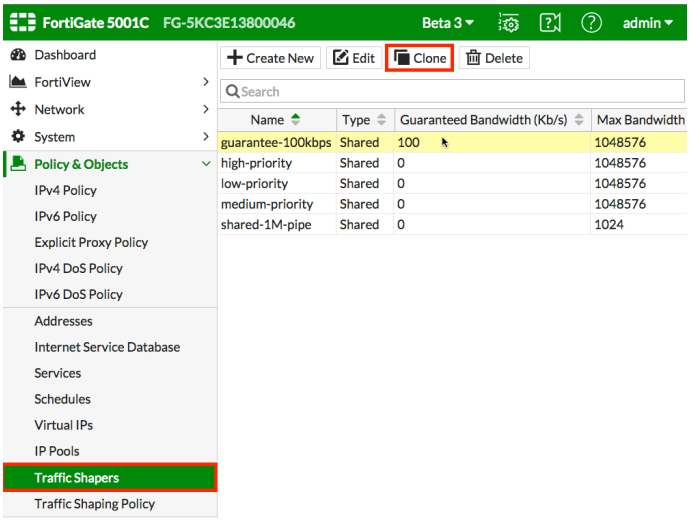
The two new attributes are `status` and `url-category`. The `status` attribute verifies whether the policy is set to enabled or disabled. The `url-category` attribute applies the shaping-policy to sessions without a URL rating when set to 0, and no web filtering is applied.

Syntax:

```
config firewall shaping-policy
   edit 1
      set status enable
      set url-category [category ID number]
```

New button added to "Clone" Shapers

You can now easily create a copy of an existing shaper by selecting the shaper and clicking the **Clone** button.



WAN link load balancing

In the same way that incoming traffic can be load balanced, outgoing or WAN traffic can also be load balanced and for the same three reasons.

1. Reduce the places in the work flow where a single point of failure can bring the process to a halt.
2. Expand the capacity of the resources to handle the required workload.
3. Have it configured so that the process of balancing the workload is automatic.

Often, it can be just as important for an organizations members to be able to access the Internet as it is for the denizens of the Internet to access the Web facing resources.

There is now a **WAN Load Balancing** feature located in the **Network** section of the GUI ("WAN LLB").

As part of the new WAN Load Balancing feature, the FortiOS 5.2 **Router > Static > Settings** GUI page has been removed. WAN Load Balancing should be used instead of the 5.2 **ECMP Load Balancing Method** settings. The 5.2 **Link Health Monitor** definitions are now only available from the CLI.

WAN links

The basis for the configuration of the virtual WAN link are the interfaces that comprise it. As interfaces are added to the "wan-load-balance" interface, they are added into the calculations that comprise the various algorithms used to do the load balancing.

- While most of the load balancing algorithms are based on equal distribution or weighted distribution, spill over does rely on which interface is first in the sequence, so this should be kept in mind when adding the interfaces.
- The interfaces in the virtual WAN link can be disabled if necessary if work needs to be done on an interface without interfering with the performance of the link.
- There is no requirement that the interfaces be those labeled on the hardware as WAN interfaces.
- In the GUI, to help analysis the effectiveness of the algorithm being used and its configuration, there is a graphic representation of the bandwidth usage of the link.

Load balancing algorithm

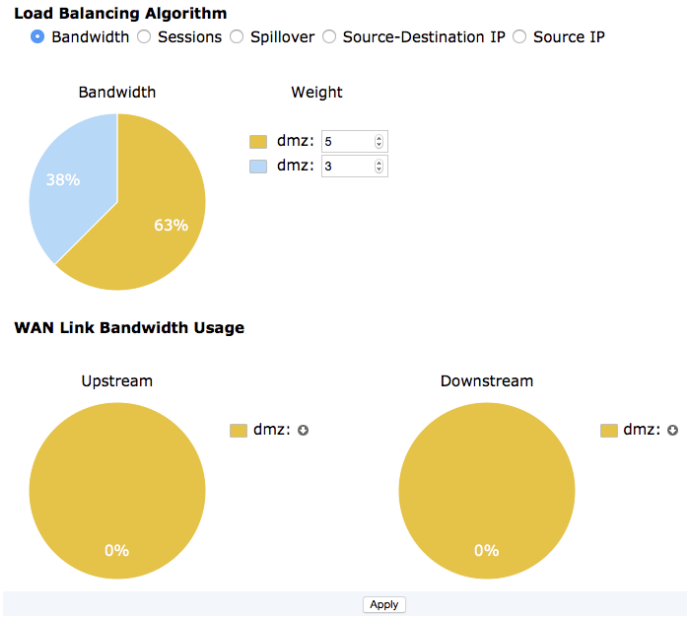
Once the interfaces involved has been configured the next step is to determine how the workload will be distributed. 5 load balancing algorithms are available to choose from.

Bandwidth

This is a very straight forward method of distributing the work load based on the amount of packets going through the interfaces. An integer value assigns a weight to each interface. These weights are used to calculate a percentage of the total bandwidth that is directed to the interface.

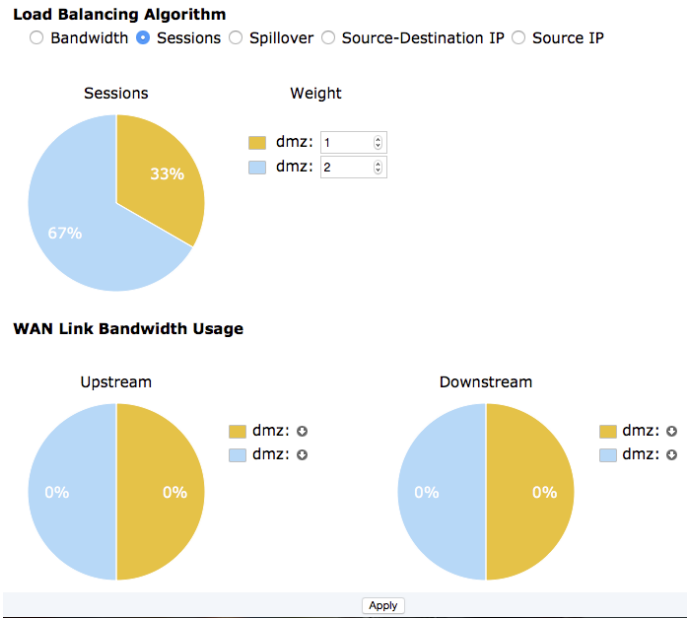
Example:

- There are 2 interfaces
- Interface #1 is assigned a weight of 5 because it is a 5 MB connection. (There is no requirement to match the weight to the capacity of the connection. It is just a simple way of optimizing the differing capacities in this case.)
- Interface #2 is assigned a weight of 3 because it is a 3 MB connection.
- The total weight is 8 so interface #1 gets 5/8 (63%) and interface #2 gets 3/8 (38%) of the traffic.



Sessions

The session algorithm is similar to the bandwidth algorithm in that it also uses an integer value to assign a weight to each interface. The difference is that the number of sessions connected is what is being measured and not the packets flowing through the interfaces.



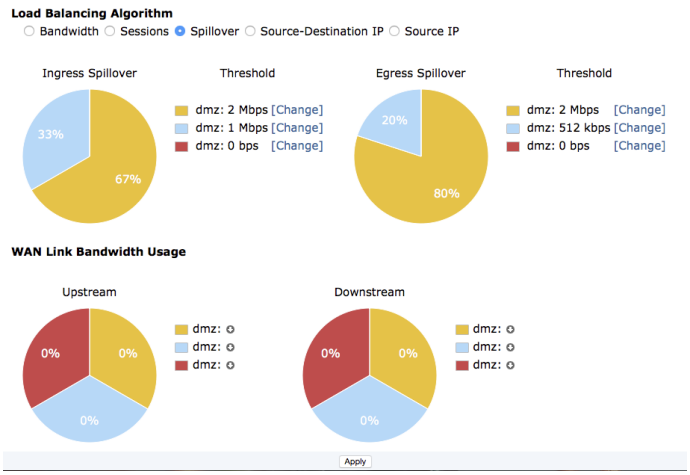
Spillover

Spillover is a method where a threshold is set for an interface (in kbps) and if the amount of traffic bandwidth exceeds the threshold any traffic bandwidth beyond that threshold is sent out through another interface.

It might be simple to just consider the outgoing or egress traffic when determining a threshold but two facts must be taken into consideration.

1. A simple request going out the interface can be responded to with significantly more data coming back from the other direction.
2. Internet connections come in a variety of configurations, many of which have different levels of allowed bandwidth capacity between the upload and download directions.

For these reasons, the FortiGate allows for the setting of both egress and ingress thresholds for bandwidth.



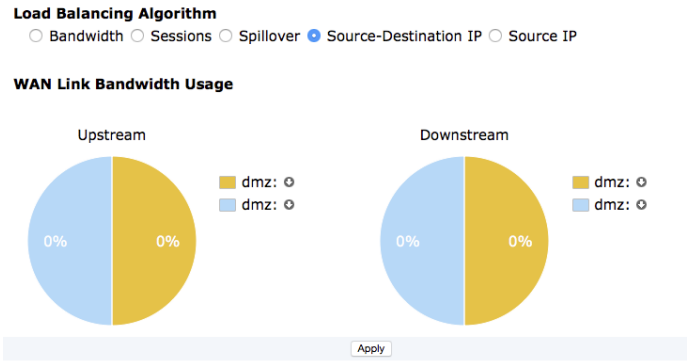
Source-destination IP

The source-destination IP algorithm tries to equally divide the traffic between the interfaces included in the virtual WAN interface. It used the connection criteria of the source and destination IP address combinations as a way of sorting the traffic.

Example:

- 10.10.10.10 to 1.1.1.2 gets sent out one interface
- Subsequent traffic going from 10.10.10.10 to 1.1.1.2 would also go out that same interface
- The next session to connect through the WAN could be either:
  - 10.10.10.27 going to 1.1.1.2
  - 10.10.10.10 going to 1.1.1.15.

Either one of the connections in the next session, even though they might match the source or the destination IP address do not match both. Traffic with the next unique combination of source and destination IP address would be sent out the other interface. It would go back and forth like this as new traffic and combinations comes in.



Source IP

The source IP address works just the same as the source-destination IP algorithm but it only concerns itself with the source IP address of the connection.

Avoid using WAN LLB in combination with asymmetric routing. Using the Bandwidth (GUI) or measure-based (CLI) load balancing algorithms can cause the routing-information (outgoing-interface) for sessions created in asymmetric routing to change in mid-session. Session-level persistence of the connection is needed to make WAN LLB effectively.

Priority rules

Some traffic requires that it come from a consistent or specific IP address to be processed properly. Because the different WAN interfaces will have different IP addresses there needs to be a way to override the unpredictability of the load balancing algorithms. This is done by using priority rules

Packets can be checked prior to being assigned an interface by the algorithm. If certain source and/or destination criteria matches the priority rules, the packets can be assigned to an outgoing interface as determined by the rule.

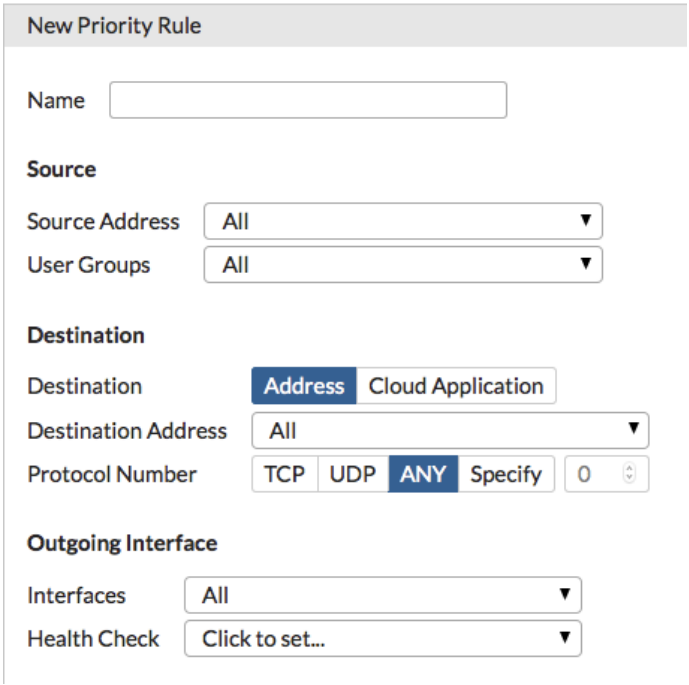
Priority rules can be configured under **Network > WAN LLB Rules**.

The source criteria that can be checked are:

- Source address
- User Group

The destination criteria that can be checked are:

- Whether it's address-based
  - Destination address
  - Protocol number
- Whether it's cloud application-based
  - The cloud application



Cloud applications

Cloud applications are a new object that can be used and configured on a FortiGate. There are a limited number of places that they can be used as a means of directing traffic and Virtual WAN links are one of them.

Estimated Bandwidth

An optional parameter has been added that allows users to set the estimated uplink and downlink bandwidths of a WAN interface.This setting is available in the GUI and the CLI. It's availability in the GUI is dependent on

context. To see the setting when editing the interface, the role of the interface must be set to WAN.

The range of the setting is from 0 to 4294967295 (effectively 2^{32}). The value is in Kbps.

In the CLI, the fields can be set by using the following syntax:

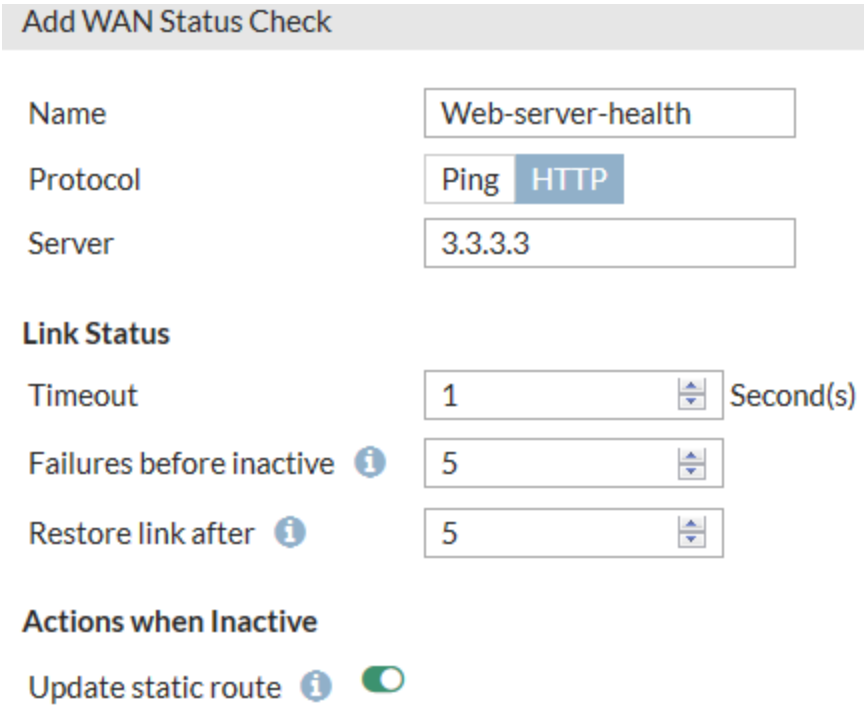
```
config system interface
   edit <wan interface>
      set estimated-upstream-bandwidth <integer from 0 - 4294967295>
      set estimated-downstream-bandwidth <integer from 0 - 4294967295>
      end
   end
```

The purpose for these settings is to work with monitoring software such as MRTG (Multi Router Traffic Grapher) to compare the estimated and real bandwith usage.This is not connected to threshold settings.

Status checking or health checking

For load balancing to be effective, there needs to be a constant monitoring of the health and status of the links that make up the virtual WAN link. Customized status checks can be configured to check on health of various aspects the traffic flow going through the link. Using either ICMP packets (PING) or HTTP requests to a designated server. Once the health reaches a specified threshold, the interface can be automatically removed from the virtual WAN link so that the algorithm is not sending traffic to a failed interface and bring down communications for a portion of the FortiGate's clientele.

To configure status or health checking go to Network > WAN Status Check and add status check profiles.



You can also configure status and health checking from the CLI. The CLI includes additional options for setting latency, jitter, and pack loss thresholds.

```
config system virtual-wan-link
```

```
set fail-detect [enable | disable]
set fail-alert-interfaces (available only if fail-detect is enabled)
config health-check
   edit [Health check name]
      set server <string>
      set protocol [ping | tcp-echo | udp-echo | http | twamp]
```

Some of the protocol options cause additional settings are made available.

http

```
      set port
      set http-get
      set http-match
```

twamp

```
      set port
      set security-mode[none | authentication]
```

The `security-mode` setting authentication generates yet another potential setting, `password`.

```
      set password
      set packet-size
```

The next settings are available for all protocols

```
      set interval <integer>
      set timeout <integer>
      set failtime [1 - 10]
      set recoverytime [1 - 10]
      set update-cascade-interface [enable | disable]
      set update-static-route [enable | disable]
      set threshold-warning-latency <integer 0-4294967295>
      set threshold-alert-latency <integer 0-4294967295>
      set threshold-warning-jitter <integer 0-4294967295>
      set threshold-alert-jitter <integer 0-4294967295>
      set threshold-warning-packetloss <integer 0-4294967295>
      set threshold-alert-packetloss <integer 0-4294967295>
      end
   end
end
```

Virtual-WAN-link improvements (365702)

Some new features have been incorporated into Virtual WAN Link to address the performance issues.

- The Virtual WAN link daemon only recalculates those services that have changed link quality.
- Removal of abnormal latency data.
- A link quality threshold has been added to prevent frequently route generation due to a small quality changes.
- Service ID field has been added
- A disable option is available for a service.
- Services in the CMDB are able to move and the order of policy routes in the kernel is based on the sequences of services in the CMDB.

Syntax for configuring a service ID

```
config system virtual-wan-link
```

```
   config service
      edit <service name>
            set id <integer between 0 - 255>
            end
```

Syntax for configuring the percentage threshold of change of link cost values that will result in a policy route generation

```
config system virtual-wan-link
   config service
      edit <service name>
            set link-cost-threshold <integer between 0 - 100000000>
            end
```

The default threshold is 10

Syntax for enabling | disabling a service

```
config system virtual-wan-link
   config service
      edit <service name>
            set status [enable | disable]
            end
```

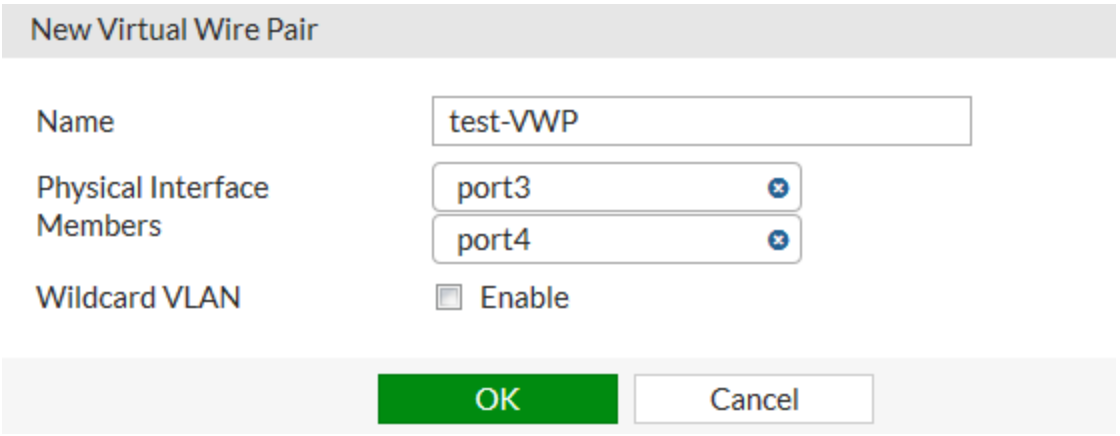
Virtual Wire Pair

This feature (276013), available in NAT and Transparent mode, replaces the Port Pair feature available in FortiOS 5.2 in Transparent mode only. When two physical interfaces are setup as a Virtual Wire Pair, they will have no IP addressing and are treated similar to a transparent mode VDOM. All packets accepted by one of the interfaces in a virtual wire pair can only exit the FortiGate through the other interface in the virtual wire pair and only if allowed by a virtual wire pair firewall policy. Packets arriving on other interfaces cannot be routed to the interfaces in a virtual wire pair. A FortiGate can have multiple virtual wire pairs.

You cannot add VLANs to virtual wire pairs. However, you can enable wildcard VLANs for a virtual wire pair. This means that all VLAN-tagged traffic can pass through the virtual wire pair if allowed by virtual wire pair firewall policies.

Adding a virtual wire pair

To add a virtual wire pair, go to **Network > Interfaces** and select **Create New > Virtual Wire Pair**. Select the interfaces to add to the virtual wire pair to, optionally enable Wildcard VLAN and select OK.



The virtual wire pair appears on the Interface list.

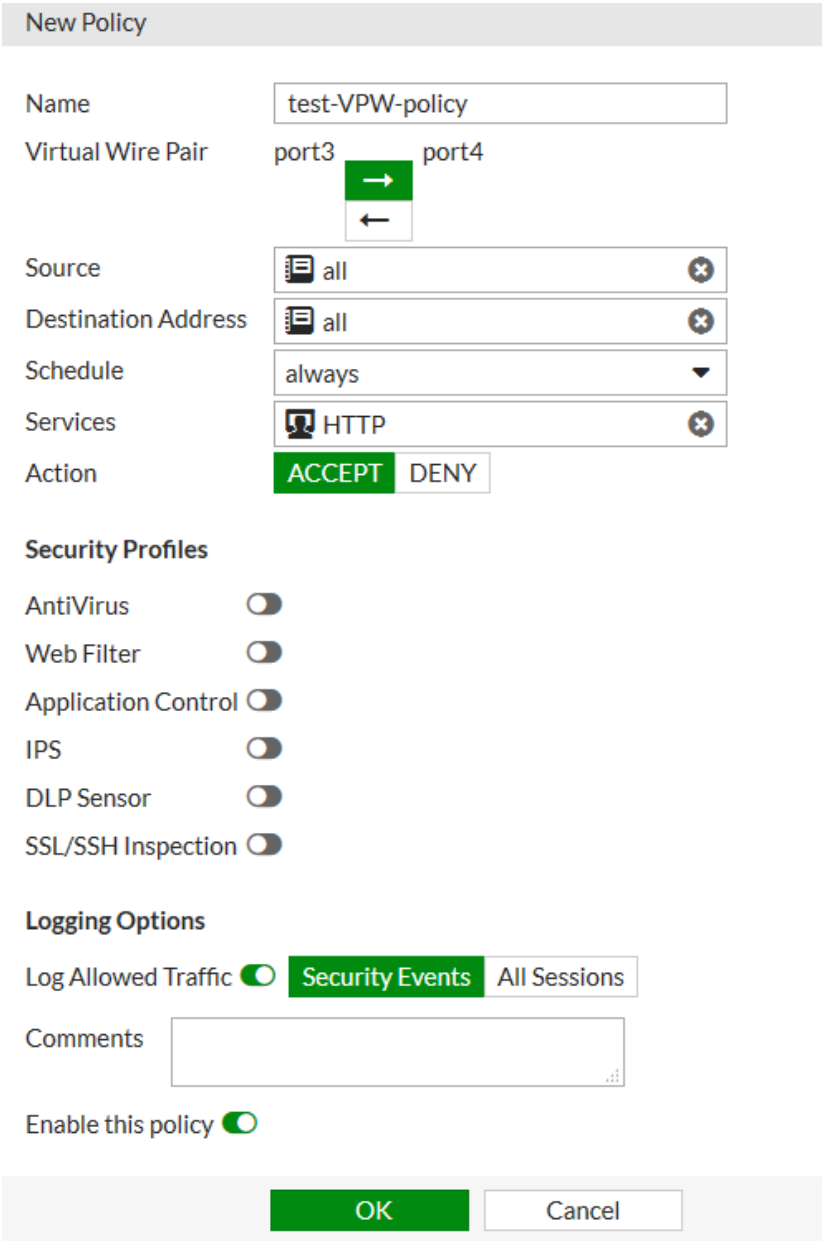
Use the following command to add a virtual wire pair from the CLI that enables the wildcard VLAN feature:

```
config system virtual-wire-pair
   edit test-VWP
      set member port3 port4
      set wildcard-vlan enable
   end
```

Assigning an interface to be part of a virtual wire pairing will remove the "role" value from the interface.

Adding a virtual wire pair firewall policy

You can add IPv4 and IPv6 virtual wire pair firewall policies. To add an IPv4 virtual wire pair firewall policy go to **Policy & Objects > IPv4 Virtual Wire Pair Policy**. Select the virtual wire pair that you want to add a policy for and select Create New. Start by configuring the direction of traffic though the policy and configure other policy settings like any firewall policy.



If you have a USB-wan interface, it will not be included in the interface list when building a wired pair.

Authentication

This chapter describes new authentication features added to FortiOS 5.4.

Support RSA-4096 bit key-length generation (380278)

In anticipation of quantum computers, RSA-4096 bit key-length CSRs can now be imported.

User authentication max timeout setting change (378085)

To accommodate wireless hotspot users authenticated on the FortiGate, the user authentication max timeout setting has been extended to 3 days (from 1 day, previously).

Changes to Authentication Settings > Certificates GUI (374980)

Added new icons for certificate types and updated formatters to use these new icons.

Support for changing a local certificate's password (297660)

Administrators can set a password through the CLI when generating a certificate request.

RADIUS CoA support (309499)

The following RADIUS CoA (Change of Authorization) CLI syntax has been added:

- Set the name of the FortiAP connected to the FortiGate as a location identifier.

CLI syntax

```
config system global
   set alias
```

- Set URL of external authentication logout server.

CLI syntax

```
config vdom
   edit root
      config wireless-controller vap
         edit <example>
            set security captive-portal
            set external-logout
```

- Set URL of external authentication logout server.

CLI syntax

```
config vdom
   edit root
      config system interface
```

```
edit <example>
   set security captive-portal
   set security-external-logout
```

- Set class name(s) included in an Access-Accept message.

CLI syntax

```
config vdom
   edit root
      config user radius
         edit accounting
            set class <"A1=aaa" "B2=bbb" "C3=ccc">
```

You can now import PKCS12 certificates from the CLI (309934)

The following CLI syntax can be entered to import a local certificate file:

CLI Syntax

```
execute vpn certificate local import tftp <file name> <tftp ip address> <file type> <Enter
    for 'cer'>|<password for 'p12'>
```

For example:

```
execute vpn certificate local import tftp FGTF-extern.p12 10.1.100.253 p12 123456
```

RADIUS Framed-IP into accounting packets (234003 189828)

RADIUS attributes, including NAS-IP-Address, Called-Station-ID, Framed-IP-Address, and Event-Timestamp, are supported.

Include RADIUS attribute CLASS in all accounting requests (290577)

RADIUS attribute CLASS in accounting requests for firewall, WiFi, and proxy authentication is now supported. RADIUS attribute CLASS is returned in Access-Accept message and it is added to all accounting requests.

- If updating to 5.4.1, see above (309499).

Certificate-related changes (263368)

Fortinet_factory certificate has been re-signed with an expiration date of 2038 and it is used instead of fortinet_factory2, which has been removed.

Improvements and changes to per-VDOM certificates (276403 267362)

The CA and local certificate configuration is now available per-VDOM. When an admin uploads a certificate to a VDOM, it will only be accessible inside that VDOM. When an admin uploads a certificate to global, it will be accessible to all VDOMs and global.

There are factory default certificates such as Fortinet_CA_SSL, Fortinet_SSL, PositiveSSL_CA, Fortinet_Wifi, and Fortinet_Factory, these certificates are moved to per-VDOM and automatically generated when a new VDOM is created.

The Fortinet_Firmware certificate has been removed and all the attributes that use Fortinet_Firmware now use Fortinet_Factory.

CLI Changes

Two new attributes `range` and `source` have been added:

`range` can be global or per-VDOM, if the certificate file is imported from global, it is a global certificate. If the certificate file is imported from a VDOM, it is VDOM certificate.

`source` can be `factory`, `user` or `fortiguard`:

`factory`: The factory certificate file with FortiOS version, this includes: Fortinet_CA_SSL, Fortinet_SSL, PositiveSSL_CA, Fortinet_Wifi, Fortinet_Factory.

`user`: Certificate file imported by the user.

`fortiguard`: Certificate file imported from FortiGuard.

```
config certificate local
   edit Fortinet_Factory
      set range global/vdom
      set source factory/user/fortiguard
   end
end
```

GUI Changes

Global and per-VDOM certificate configuration includes **view details**, **download**, **delete**, and **import** certificate.

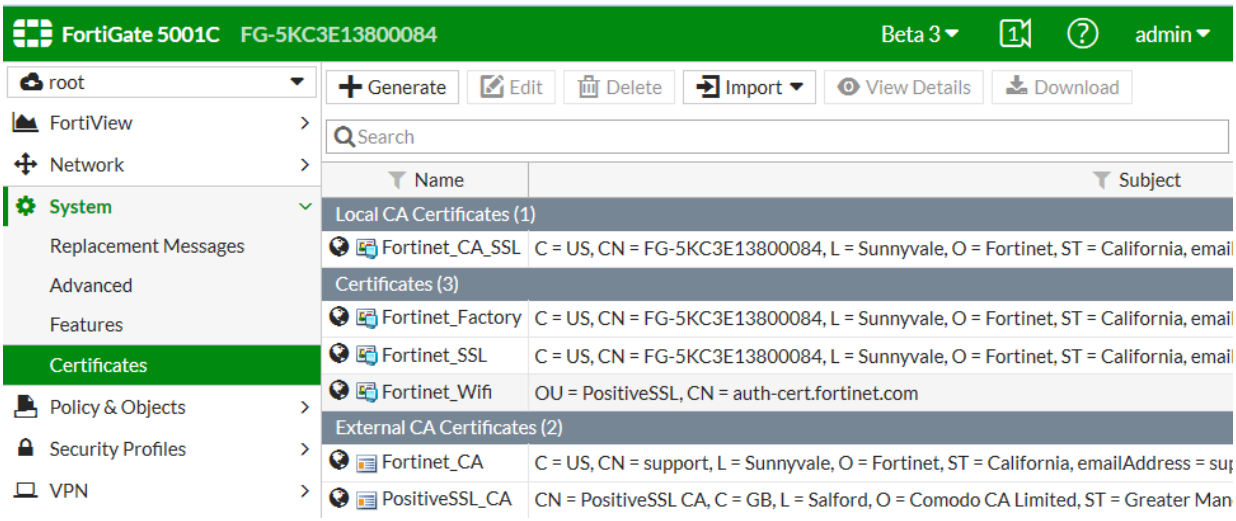
A **Source** and a **Status** columns have been added.

A global icon for **Name** column when VDOMs are enabled is added to show that the certificate is global.

A new VDOM now has the following default certificates: Fortinet_CA_SSL, Fortinet_Factory, Fortinet_SSL, Fortinet_Wifi, Fortinet_CA, and PositiveSSL_CA. These certificates are created automatically when the VDOM is created and every VDOM will have its own individual versions of these certificates.

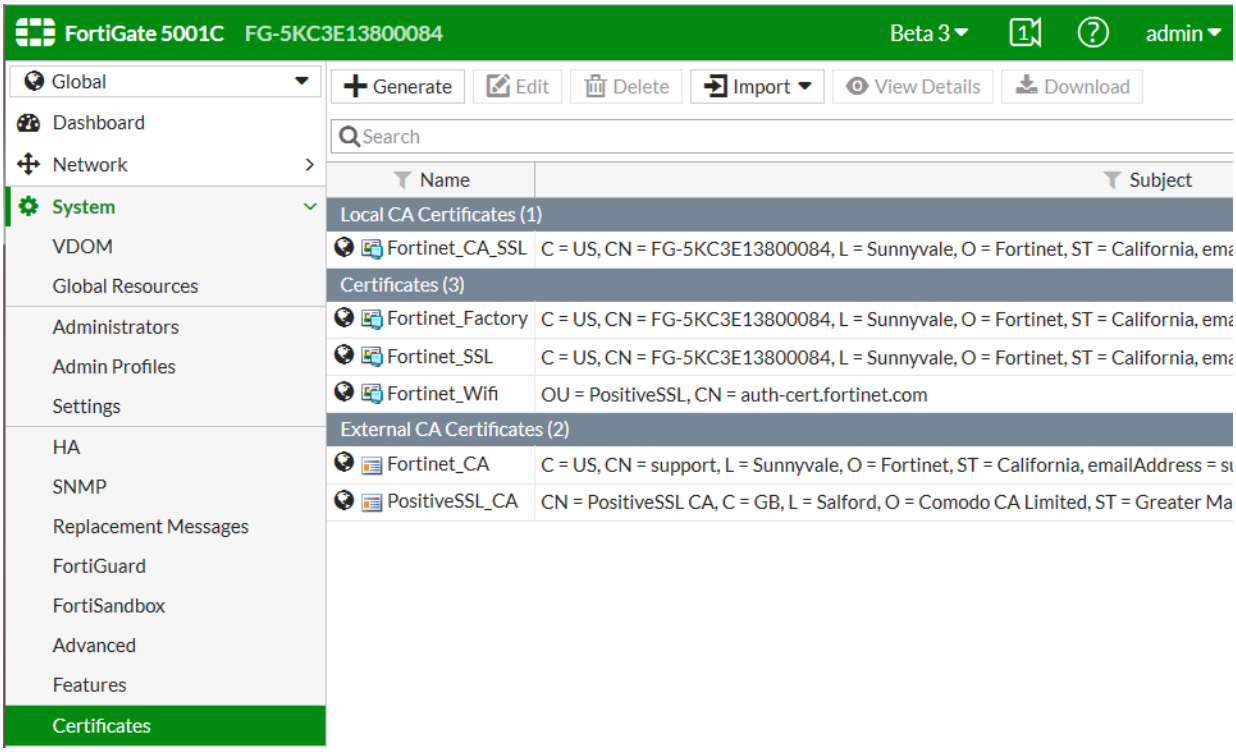
The Fortinet_firmware certificate has been removed. All default configurations that formerly used the Fortinet_ firmware certificate now use the Fortinet_Factory certificate.

Default root VDOM certificates



Certificates with the same names are also available from the global configuration. These are generated when you turn on VDOMs.

Default global certificates



Adding certificates to VDOMs and to the global configuration

If an administrator adds a certificate to a VDOM the certificate will only be available for that VDOM. If an administrator adds a certificate to the global configuration it will available for all VDOMs.

Guest user enhancements (291042)

The password policy profile for guest Admin is improved. This is a CLI only configuration as following:

```
config system password-policy-guest-admin
   status enable/disable Enable/disable password policy.
   apply-to guest-admin-password Guest admin to which this password policy applies.
   minimum-length  Minimum password length.
   min-lower-case-letter  Minimum number of lowercase characters in password.
   min-upper-case-letter  Minimum number of uppercase characters in password.
   min-non-alphanumeric Minimum number of non-alphanumeric characters in password.
   min-number  Minimum number of numeric characters in password.
   change-4-characters enable/disable Enable/disable changing at least 4 characters for new password.
   expire-status enable/disable Enable/disable password expiration.
   reuse-password enable/disable  Enable/disable reuse of password.
end
```

RADIUS CoA for user, user-group and captive-portal authentication (RFC 5176) (274813 270166)

RADIUS Change of Authorization (CoA) is a common feature in user authentication. User, user-group and captive-portal authentication now supports RADIUS CoA, when the back end authentication server is RADIUS.

The main use case of this feature is with external captive portal, it can be used to disconnect hotspot users when their time, credit or bandwidth had been used up.

- If updating to 5.4.1, see above (309499).

RSSO: Enable or disable overriding old attribute value when a user logs in again (possibly on a different device) (278471)

When receiving a new start message with different group name for the same user and different IP address such as the scenario of a mobile device roaming, the original design is to override all group name information to the latest group name received from the latest start message.

This new feature adds an option to disable this override when needed. The default behavior keeps the original design.

CLI changes

Add an option to enable or disable overriding SSO attribute value.

Syntax

```
config user radius
   edit <My_Rsso>
   set rsso enable
```

```
    set sso-attribute-value-override enable/disable // Enable/Disable override old attribute value
        with new value for the same endpoint.
end
```

FSSO supports Microsoft Exchange Server (270174)

FSSO supports monitoring Microsoft Exchange Server. This is useful for situation that the user use the domain account to access their email, but client device might or might not be in the domain. Support for Exchange server is configured on the Back-end FSSO collector agent under **Advanced Settings** > **Exchange Server**.

Select **Add** and enter the following information and select **OK**.

Domain Name	Enter your domain name.
Server IP/Hostname	Enter the IP address or the hostname of your exchange server.
Polling forwarded event log	This option for scenarios when you do not want that CA polls the Exchange Server logs directly. In this case you need to configure event log forwarding on the Exchange server. Exchange event logs can be forwarded to any member server. If you enable this, instead of the IP of the Exchange server configured in the previous step, you must then configure the IP of this member server. CA will then contact the member server.
Ignore Name	Because CA will also check Windows log files for logon events and when a user authenticates to Exchange Server there is also a logon event in Windows event log, which CA will read and this will overwrite the Exchange Server logon event (ES-EventLog) on CA. So it is recommended to set the ignore list to the domain the user belongs to. To do so, enter the domain name in the **Ignore Name** field and select **Add**.

PCI DSS compliance

This chapter describes new PCI DSS compliance features added to FortiOS 5.4.

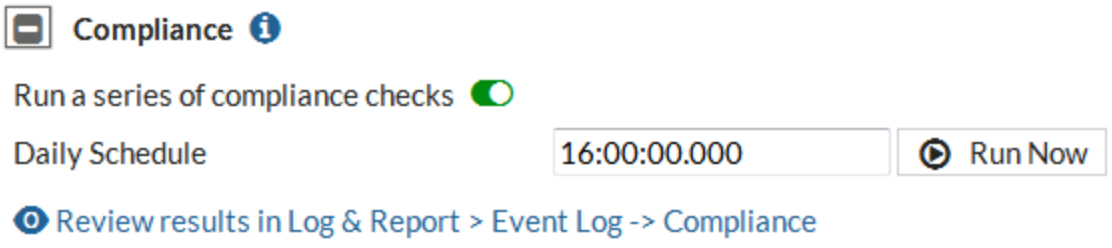
Vulnerability Scanning has been removed (293156)

Vulnerability scanning can now be done from FortiClient.

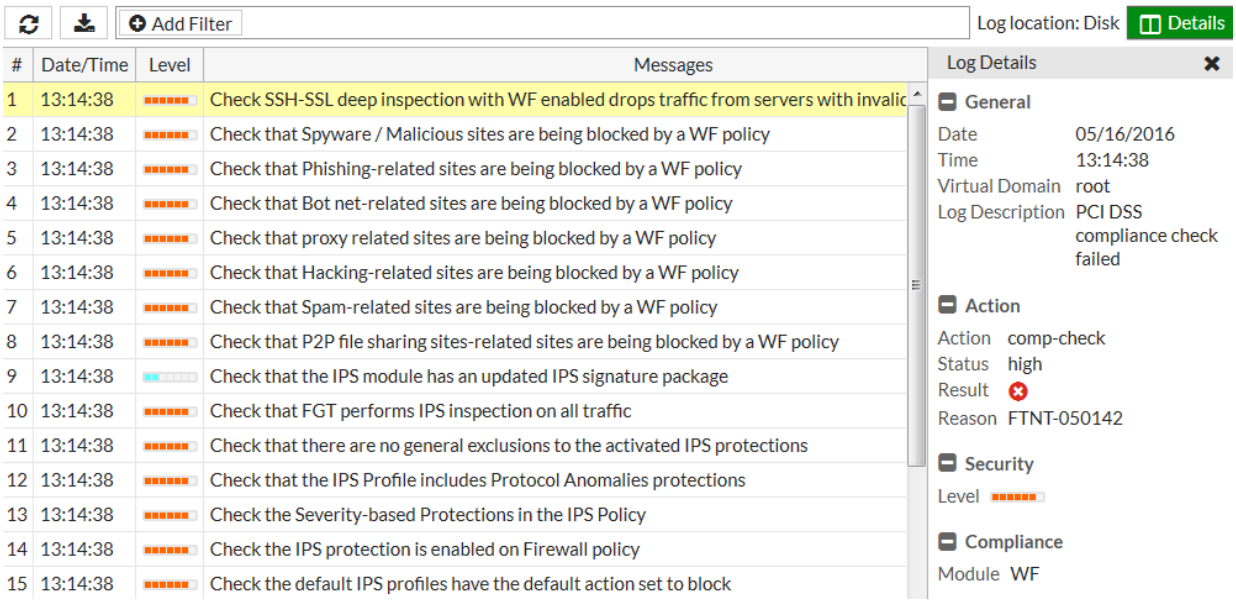
PCI DSS Compliance Check Support (270014)

FortiOS 5.4 allows you to run a compliance check either on demand or according to a schedule that automatically checks PCI DSS compliance at the global or VDOM level. The compliance check determines whether the FortiGate is compliant with each PCI DSS requirement by displaying an 'X' next to the non-compliant entries in the GUI logs.

Go to **System > Advanced > Compliance**, turn on compliance checking and configure a daily time to run the compliance check. Or you can select **Run Now** to run the compliance check on demand.



Go to **Log & Report > Compliance Events** to view compliance checking log messages that show the results of running compliance checks.



Device identification

This chapter describes new Device Identification features added to FortiOS 5.4.

Passive detection of FortiFone, FortiCam and routers (304068)

Two new device groups types have been created in order to automatically provision FortiFone and FortiCam into different VLANs. Previously any FortiFone devices, and any FortiCam devices with a Fortinet MAC address, would have been included in the "Fortinet Devices" type.

These new device groups are found under **User & Device > Device List**.

802.1x Mac Authentication Bypass (197218)

Some FortiGate models contain a hardware switch. On the hardware switch interface, 802.1X authentication is available. You might want to bypass 802.1X authentication for devices such as printers that cannot authenticate, identifying them by their MAC addresses.

In the CLI, enable MAC authentication bypass on the interface:

```
config system interface
   edit "lan"
      set ip 10.0.0.200 255.255.255.0
      set security-mode 802.1X
      set security-mac-auth-bypass enable
      set security-groups "Radius-group"
   end
```

The devices that bypass authentication have entries in the RADIUS database with their MAC address in the User-Name and User-Password attributes instead of user credentials.

Vulnerability Scan status change(293156)

The FortiGate will no longer function as a vulnerability scanner, even in CLI mode. Vulnerability scans / assessments will handled by the FortiClient software.

FortiFone devices are now identified by FortiOS (289921)

FortiFone devices are now identified by FortiOS as **Fortinet FON**.

Support for MAC Authentication Bypass (MAB) (197218)

MAC Authentication Bypass allows devices without 802.1X capability (printers and IP phones for example) to bypass authentication and be allowed network access based on their MAC address. This feature requires RADIUS-based 802.1X authentication in which the RADIUS server contains a database of authorized MAC addresses.

MAC Authentication Bypass is configurable only in the CLI and only on interfaces configured for 802.1X authentication. For example:

```
config system interface
   edit "lan"
      set ip 10.0.0.200 255.255.255.0
      set vlanforward enable
      set security-mode 802.1X
      set security-mac-auth-bypass enable
      set security-groups "Radius-group"
   end
end
```

MAC Authentication Bypass is also available on WiFi SSIDs, regardless of authentication type. It is configurable only in the CLI. You need to enable the `radius-mac-auth` feature and specify the RADIUS server that will be used. For example:

```
config wireless-controller vap
   edit "office-ssid"
      set security wpa2-only-enterprise
      set auth usergroup
      set usergroup "staff"
      set radius-mac-auth enable
      set radius-mac-auth-server "ourRadius"
   end
end
```

Active device identification (279278)

Hosts whose device type cannot be determined passively are actively scanned using the same techniques as the vulnerability scan. This active scanning is enabled by default on models that support vulnerability scanning. You can turn off Active Scanning on any interface. In the GUI, go to the interface's page in **Network > Interfaces**.

CLI Syntax:

```
config system interface
   edit port1
      set device-identification enable
      set device-identification-active-scan disable
   end
```

Device Page Improvements (Detected and custom devices) (280271)

Devices are now in two lists on the **User & Device** menu. Detected devices are listed in the **Device List** where you can list them alphabetically, by type, or by interface. On the **Custom Devices and Groups** page you can

- create custom device groups
- predefine a device, assigning its device type and adding it to custom device groups

Device offline timeout is adjustable (269104)

A device is considered offline if it has not sent any packets during the timeout period. Prior to FortiOS 5.4, the timeout value was fixed at 90 seconds. Now the timeout can be set to any value from 30 to 31 536 000 seconds (365 days). The default value is 300 seconds (5 minutes). The timer is in the CLI:

```
config system global
   set device-idle-timeout 300
end
```

Improved detection of FortiOS-VM devices (272929)

A FortiGate-VM device is an instance of FortiOS running on a virtual machine (VM). The host computer does not have the Fortinet MAC addresses usually used to detect FortiGate units. Device detection now has two additional ways to detect FortiGate-VMs:

- the FortiGate vendor ID in FortiOS IKE messages
- the FortiGate device ID in FortiGuard web filter and spamfilter requests

Custom avatars for custom devices (299795)

You can upload an avatar for a custom device. The avatar is then displayed in the GUI wherever the device is listed, such as FortiView, log viewer, or policy configuration. To upload an avatar image,click Upload Image on the New Device or Edit Device page of **User & Device > Custom Devices & Groups**. The image can be in any format your browser supports and will be automatically sized to 36 x 36 pixels for use in the FortiGate GUI.

Diagnose command changes

This chapter describes new diagnose features added to FortiOS 5.4.

Antivirus diagnose command changes (299408)

There is a new diagnose command that shows antivirus database information.

```
diagnose antivirus database-info
```

This command shows:

- virus count
- grayware count
- signature count for antivirus databases.

The following antivirus diagnose commands have been removed:

```
diagnose antivirus heuristic showthreshold
diagnose antivirus heuristic showrules
diagnose antivirus virus list
```

Diagnose hardware test command supported on FortiGate-300D and 500D (302021)

The `diagnose hardware test` command with all of it options, replaces the functionality of the HQIP test firmware. Now hardware tests can be performed without installing an alternate firmware on the device. A listing of the options to this command can be found at http://wiki.diagnose.fortinet.com/index.php/diagnose_hardware_test.

This feature has been available on the E series FortiGates with 5.4 . It is now available in 5.4.1 on the FortiGate 300D and 500D models.

Option to skip interfaces in diagnose hardware test command (310778)

This diagnostic option allow specific interfaces to be skipped when perform performance tests on a FortiGate.

```
diag hardware test skip
```

One of the advantages of this method of hardware testing compared to the HQIP test, is that the device does not have to be shut down to run the tests. This advantage would be nullified if the running of the test brought down the functionality of the FortiGate. By skipping interfaces, tests can be run without impacting traffic.

This option of the diagnose hardware test command can be used with the following options.

`clear` - Clears the list of interfaces to be skipped during testing

`show` - Shows the current list of interfaces that are skipped during testing

`<interface>` - Includes an interface to the list of interfaces that are skipped during testing. This function is cumulative. Using the command to skip another interface does not replace the previous interface, it adds an additional one.

New diagnose sys top option (302607)

You can now enter the `diagnose sys top` command and include an option to control the number of times the command refreshes the listed processes before exiting.

The syntax for the command is now diagnose sys top <time between intervals> <number of processes> <number of intervals before quiting>

For example the following command displays 20 lines of output (the default), refreshes the display every 5 seconds (the default), and exits after refreshing the display 3 times.

```
diagnose sys top 5 20 3
```

By default the process list refreshes until you press "ctrl-c" or "q" to interrupt it. Setting a refresh limit is useful when you are using the command to gather information for Fortinet Support or for other reasons where you don't need the display to keep refreshing.

New diagnose command to display more detailed geographic information (310567)

Previously, there was a command that could return the country that an IPv4 address is located in.

```
diagnose geoip ip2country x.x.x.x
```

Now there is a command that will provide more granular information about the geographic location of an IPv4 address. I.e.not just the country, but the city or town as well.

```
diagnose geoip geoip-query x.x.x.x
```

Most diagnose sys dashboard commands removed (129248)

The `diagnose sys dashboard reset` command is still available.

FortiView network segmentation tree diagnose command (286116)

Enter `diagnose sys nst {downstream | query}` to display information about the FortiView network segmentation tree,

`downstream` shows connected downstream FortiGates.

`query` query the network segmentation tree.

Changes to diagnose hardware deviceinfo disk command (271816)

Extraneous information has been removed from the `diagnose hardware deviceinfo disk` command output and some field names have been changed.

Display the CLI schema (256892)

You can use these diagnose commands to display the CLI schema:

Enter `diagnose web-ui cli-schema` to display the entire schema.

Enter `diagnose web-ui cli-schema <branch-name>` to display just a single branch of the tree. For example, enter `diagnose web-ui cli-schema firewall policy` to dipslay the firewall policy schema.

New NP4 DDR diagnose command (261258)

Use the `diagnose np4 ddr` command to debug NP4 DDR settings.

```
diagnose npu np4 dqs-write
diagnosis npu np4 dqs-read <dev-id>
diagnosis npu np4 crps-write <dev-id> <CRPS>
diagnosis npu np4 crps-read <dev-id>
```

Ekahau site survey information to diagnose wireless wlac command (267384)

The output of the `diagnose wireless wlac` command includes information about Ehahau site survey results.

Port kernel profiling (237984)

Use the `diagnose sys profile {start | stop | show | sysmap | cpumask | module}` command to display port kernel profiling information.

`start` start kernel profiling data

`stop` copy kernel profiling data

`show` show kernel profiling result

`sysmap` show kernel sysmap

`cpumask` profile which CPUs

`module` show kernel module

Use the following steps:

1. set cpu mask first
2. run start command
3. run stop command to read the profiling data and analyze
4. run show command to show the result
5. set cpu mask 00 to stop profiling

List the most recently modified files (254827)

Use the `diagnose sys last-modified-files {path | number}` command to list the last (by default 10) modified files in a given directory.

`path` file system path from which to list modified files (default = /data).

`number` number of files to list (default = 10).

LTE modem diagnose command (279545)

```
dia test application lted <id>
```

Where <id> can be:

1. Show device info
2. Show data session connection status
3. Test connection
4. Test disconnection
5. Get signal strength
6. Get IP address
7. Get IP address and DNS server
8. Get SIM card status
9. Restart LTE device
10. Show LTED status
11. Resync LTED status
12. Check USB LTE/WiMAX configuration conflict
13. Stop monitor
14. Start monitor
15. List supported AT commands
16. Disable RF(Should stop monitor first)
17. Enable RF(Should start monitor first)
18. Get MIP information
19. Show current network service mode
20. Show current Channel/Bandclass
21. Show activation status
22. Show SIM status
23. Show registration status
24. Get IMEI
25. Get ICCID

New diagnose sys botnet command

Use the diagnose sys botnet {stat | list | find | flush | reload | file} command to display information about botnet information in the kernel and to flush and reload botnet information into the kernel.

`stat` the number of botnet entries in the kernel.

`list` list the botnet entries.

`find` find a botnet entry by ip address, port number, protocol etc.

`flush` flush botnet entries from the kernel.

`reload` reload botnet file into the kernel

`file` botnet file diagnostics.

Example command output:

```
diagnose sys botnet list
Read 10 botnet entry:
0. proto=TCP ip=0.175.57.24, port=80, name_id=8, rule_id=48
1. proto=UDP ip=1.22.117.135, port=16470, name_id=0, rule_id=32
2. proto=UDP ip=1.22.177.28, port=16465, name_id=0, rule_id=32
3. proto=UDP ip=1.22.213.38, port=16465, name_id=0, rule_id=32
4. proto=UDP ip=1.23.81.128, port=16465, name_id=0, rule_id=32
5. proto=UDP ip=1.23.82.125, port=16465, name_id=0, rule_id=32
6. proto=UDP ip=1.23.83.46, port=16465, name_id=0, rule_id=32
7. proto=UDP ip=1.23.83.138, port=16465, name_id=0, rule_id=32
8. proto=UDP ip=1.23.89.60, port=16465, name_id=0, rule_id=32
9. proto=UDP ip=1.23.128.18, port=16470, name_id=0, rule_id=32
```

Unquarantine all quarantined FortiClient devices (284146)

You can use the `diagnose endpoint registration unquarantine all` command to unquarantine all quarantined FortiClient devices.

Port HQIP to FortiOS using standard diagnose CLI (290272)

On FortiGate E series models, instead of downloading a special HQIP image to run hardware tests you can use the following command .

`diagnose hardware test`, followed by one of the following options:

- `bios` - perform BIOS related tests.
- `system` - perform system related tests.
- `usb` - perform USB related tests.
- `button` - perform button related tests.
- `cpu` - perform CPU related tests.
- `memory` - perform memory related tests.
- `network` - perform network related tests.
- `disk` - perform disk related tests.
- `led` - perform LED related tests.

- `wifi` - perform wifi related tests.
- `suite` - runthe HQIP test suite.
- `setting` - change test settings.
- `info` - show test parameters.

Access Control List (ACL) diagnose command (0293399)

Use the `diagnose firewall acl {counter | counter6 | clearcounter | clearcounter6}` command to display information about the access control list feature:

`counter` Show number of packets dropped by ACL.

`counter6` Show number of packets dropped by IPv6 ACL.

`clearcounter` Clear ACL packet counter.

`clearcounter6` Clear the IPv6 ACL packet counter.

New traffic test functionality (279363)

```
diagnose traffictest {show | run -h arg | server-intf | client-intf | port | proto}
```

Where -h arg can be

-f, --format [kmgKMG] format to report: Kbits, Mbits, KBytes, MBytes

-i, --interval # seconds between periodic bandwidth reports

-F, --file name xmit/recv the specified file

-A, --affinity n/n,m set CPU affinity

-V, --verbose more detailed output

-J, --json output in JSON format

-d, --debug emit debugging output

-v, --version show version information and quit

-h, --help show this message and quit

-b, --bandwidth #[KMG][/#] target bandwidth in bits/sec (0 for unlimited) (default %d Mbit/sec for UDP, unlimited for TCP) (optional slash and packet count for burst mode)

-t, --time # time in seconds to transmit for (default %d secs)

-n, --bytes #[KMG] number of bytes to transmit (instead of -t)

-k, --blockcount #[KMG] number of blocks (packets) to transmit (instead of -t or -n)

-l, --len #[KMG] length of buffer to read or write (default %d KB for TCP, %d KB for UDP)

-P, --parallel # number of parallel client streams to run

-R, --reverse run in reverse mode (server sends, client receives)

-w, --window #[KMG] TCP window size (socket buffer size)

-C, --linux-congestion <algo> set TCP congestion control algorithm (Linux only)

-M, --set-mss # set TCP maximum segment size (MTU - 40 bytes)

-N, --nodelay set TCP no delay, disabling Nagle's Algorithm

-4, --version4 only use IPv4

-6, --version6 only use IPv6

-S, --tos N set the IP 'type of service'

-L, --flowlabel N set the IPv6 flow label (only supported on Linux)

-Z, --zerocopy use a 'zero copy' method of sending data

-O, --omit N omit the first n seconds

-T, --title str prefix every output line with this string

--get-server-output get results from server

[KMG] indicates options that support a K/M/G suffix for kilo-, mega-, or giga-

New switch error counters for diagnose hardware deviceinfo nic command (285730)

New diag hardware deviceinfo flash command (300119)

To display flashprogram/erase count on 30D/60D/30E/50E/51E Platforms.

Explicit web proxy

This chapter describes new explicit web proxy features added to FortiOS 5.4.

Support Kerberos and NTLM authentication (370489)

FortiGate now recognizes the client's authentication method from the token and selects the correct authentication scheme to authenticate successfully.

CLI syntax

```
config firewall explicit-proxy-policy
   edit <example>
      set active-auth-method [ntlm | basic | digest | negotiate | none]
   end
```

Explicit Web Proxy WISP support improvements (309388 309236)

The following Explicit Web Proxy WISP CLI syntax has been changed and added:

- Changed web-proxy wisp to table object and added outgoing-ip.

CLI syntax

```
config web-proxy
   set server-ip // WISP server IP address
   set server-port // WISP server port (1 - 65535)
```

- In the web filter profile, added WISP servers and WISP algorithm.

CLI syntax

```
config webfilter profile
edit <example>
set wisp-servers // WISP servers
set wisp-algorithm // WISP server selection algorithm
```

Improvements to explicit web proxy policy page (305817)

Explicit proxy URL categories show description next to their numerical values in the CLI. Also, all categories for **URL Category** are available in the GUI.

Explicit web proxy Kerberos authentication support (297503)

The following web proxy Kerberos authentication CLI syntax has been added:

CLI syntax

```
config user krb-keytab
edit <example>
```

```
set principal // Kerberos service principal
set ldap-server // LDAP server name
set keytab // base64 coded keytab
```

Explicit proxy, Web Caching, and WAN Optimization are not supported for Flow-based VDOMs (274748)

Explicit proxy, web caching, and WAN optimization have been removed from the GUI in a Flow-based VDOM.

Explicit proxy support for base64 encoded X-Authenticated-Groups and X-Authenticated-User HTTP headers (356979)

Data for http header-names X-Authenticated-Groups and X-Authenticated-User are decoded before further processing.

New explicit proxy firewall address types (284753)

New explicit proxy firewall address types improve granularity over header matching for explicit web proxy policies. You can enable this option using the **Show in Address List** button on the Address and Address Group New/Edit forms under **Policy & Objects > Addresses**.

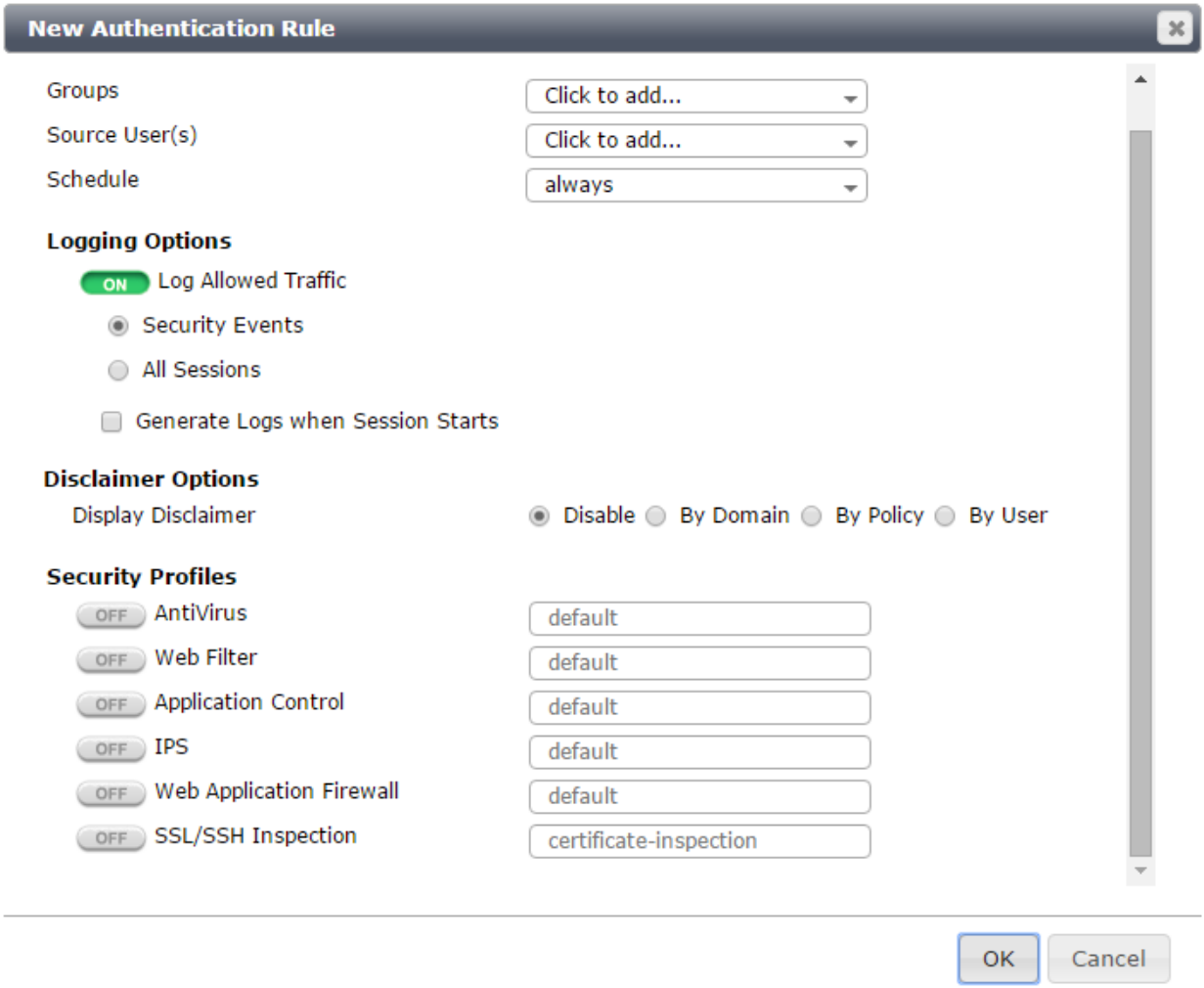
The following new address types have been added:

- **URL Pattern** - destination address
- **Host Regex Match** - destination address
- **URL Category** - destination address (URL filtering)
- **HTTP Method** - source address
- **User Agent** - source address
- **HTTP Header** - source address
- **Advanced (Source)** - source address (combines User Agent, HTTP Method, and HTTP Header)
- **Advanced (Destination)** - destination address (combines Host Regex Match and URL Category)

Disclaimer messages can be added to explicit proxy policies (273208)

Disclaimer options are now available for each explicit proxy policy or split policy of ID-based policy. This feature allows you to create user exceptions for specific URL categories (including warning messages) based on user groups.

The **Disclaimer Options** are configured under **Policy & Objects > Explicit Proxy Policy**. You can also configure a disclaimer for each Authentication Rule by setting **Action** to **Authenticate**.



Disclaimer explanations

- **Disable:** No disclaimer (default setting).
- **By Domain:** The disclaimer will be displayed on different domains. The explicit web proxy will check the referring header to mitigate the javascript/css/images/video/etc page.
- **By Policy:** The disclaimer will be displayed if the HTTP request matches a different explicit firewall policy.
- **By User:** The disclaimer will be displayed when a new user logs on.

Firewall virtual IPs (VIPs) can be used with Explicit Proxy policies (234974)

The explicit web-proxy will now accept VIP addresses for destination address. If an external IP matches a VIP policy, the IP is changed to the mapped-IP of the VIP.

Implement Botnet features for explicit policy (259580)

The option `scan-botnet-connections` has been added to the firewall explicit proxy policy.

Syntax:

```
config firewall explicit-proxy-policy
   edit <policyid>
      set scan-botnet-connections [disable/block/monitor]
end
```

where:

`disable` means do not scan connections to botnet servers.

`block` means block connections to botnet servers.

`monitor` means log connections to botnet servers.

Add HTTP.REFERRER URL to web filter logs (260538)

Added support for the referrer field in the HTTP header on webfilter log, this field along with others in the HTTP header are very useful in heuristic analysis /search for malware infected hosts.

Adding guest management to explicit web proxy (247566)

Allow user group with type **Guest** to be referenced in explicit-proxy-policy.

Firewall

This chapter describes new firewall features added to FortiOS 5.4.

Multiple interfaces or ANY interface can be added to a firewall policy (288984)

This feature can be enabled or disabled in the GUI by going to the **System > Feature Select** page and toggling **Multiple Interface Policies**.

When selecting the **Incoming** or **Outgoing** interface of a policy, there are a few choices:

- The ANY interface (choosing this will remove all other interfaces)
- A single specific interface
- multiple specific interfaces (can be added at the same time or one at a time)

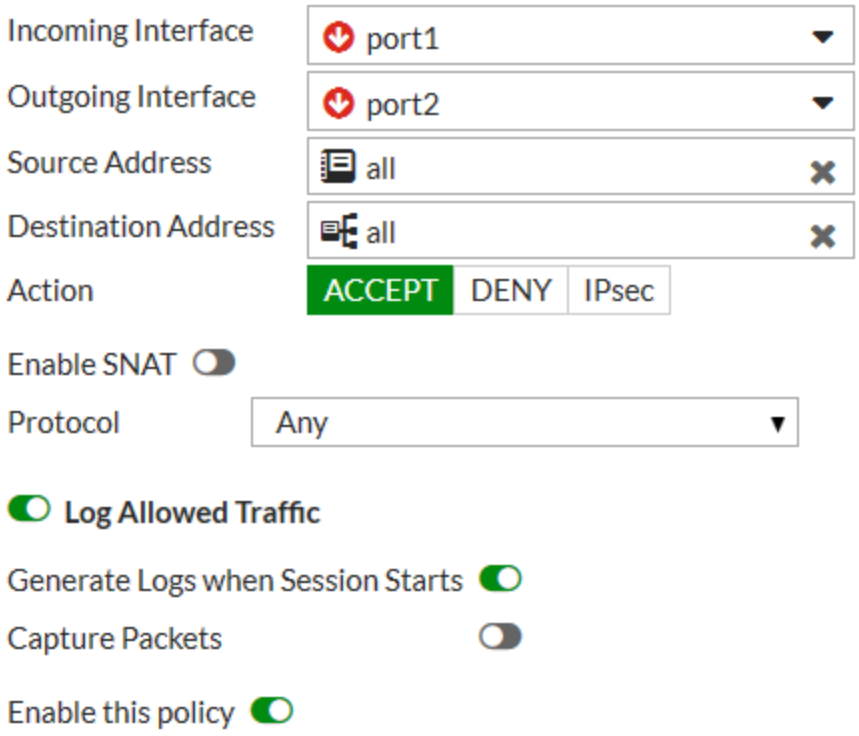
  The GUI is intuitive and straightforward on how to do this. Click on the "+" symbol in the interface field and then select the desired interfaces from the side menu. There are a couple of ways to do it in the CLI:

1. Set the interfaces all at once:
```
config firewall policy
   edit 0
      set srcintf wan1 wan2
      end
```
2. Set the first interface and append additional ones:
```
config firewall policy
   edit 0
      set srcintf wan1
      append srcintf wan2
      end
```

Multicast policy page changes (293709 305114)

The multicast policy GUI page has been updated to the new GUI look and feel. Some functionality has also been changed.

- The DNAT option has been removed from the GUI but is still in the CLI, you can set the action to IPsec, and if you select Log Allowed Traffic you can also select a few logging options.
- The Multicast policy page loads faster.



Policy objects dialogs updated to new GUI style (354505)

To avoid confusion, the default value for "day" is no longer Sunday. In the GUI, none of the day options are selected.

Display change in Policy listing (284027)

Alias names for interfaces, if used now appear in the headings for the Interface Pair View or what used to be called the Section View.

RPC over HTTP traffic separate (288526)

How protocol options profiles and SSL inspection profiles handle RPC (Remote Procedure Calls) over HTTP traffic can now be configured separately from normal HTTP traffic.

CLI syntax changes

```
config firewall profile-protocol-options
   edit 0
      set rpc-over-http {disable | enable}
   end

config firewall ssl-ssh-profile
   edit deep-inspection
      set rpc-over-http {disable | enable}
```

```
end
```

Disable Server Response Inspection supported (274458)

Disable Server Response Inspection (DSRI) option included in Firewall Policy (CLI only) to assist performance when only using URL filtering as it allows the system to ignore the http server responses.

CLI syntax for changing the status of the DSRI setting:

```
conf firewall policy|policy6
   edit NNN
      set dsri enable/disable
      end

conf firewall interface-policy|interface-policy6
   edit NNN
      set dsri enable/disable
      end

conf firewall sniffer
   edit NNN
      set dsri enable/disable
      end
```

Policy counter improvements (277555 260743 172125)

- implicit deny policy counter added
- first-hit time tracked for each policy
- "Hit count" is tracked for each policy (total number of new sessions since last reset)
- Most counters now persist across reboots

Bidirectional Forwarding Detection (BFD) (247622)

Bidirectional Forwarding Detection (BFD) protocol support has been added to Protocol Independent Multicast (PIM), to detect failures between forwarding engines.

TCP sessions can be created without TCP syn flag checking (236078)

A Per-VDOM option is available to enable or disable the creation of TCP sessions without TCP SYN flag checking

Mirroring of traffic decrypted by SSL inspection (275458)

This feature sends a copy of traffic decrypted by SSL inspection to one or more FortiGate interfaces so that it can be collected by raw packet capture tool for archiving and analysis.

This feature is available if the inspection mode is set to flow-based. Use the following command to enable this feature in a policy. The following command sends all traffic decrypted by the policy to the FortiGate port1 and port2 interfaces.

```
conf firewall policy
   edit 1
      set ssl-mirror enable/disable
      set ssl-mirror-intf port1 port2
   next
```

Support for full cone NAT (269939)

Full cone NAT maps a public IP address and port to a LAN IP address and port. This means that a device on the Internet can send data to the internal LAN IP address and port number by directing it a the external IP address and port number. Sending to the correct IP address but a different port will cause the communication to fail. This type of NAT is also known as port forwarding.

Full cone NATing is configured only in the CLI. It is done by properly configuring an IP pool for the NATing of an external IP address. The two important settings are:

- `set type` - it must be set to `port-block-allocation` to use full cone
- `set permit-any-host` - enabling it is what enables full cone NAT

An example fo the IP pool configuration would be:

```
config firewall ippool
   edit "full_cone-pool1"
      set type port-block-allocation
      set startip 10.1.1.1
      set endip 10.1.1.1
      set permit-any-host enable
      end
```

Enable or disable inspecting IPv4 and IPv6 ICMP traffic (258734)

There is now a system setting that determines if ICMP traffic can pass through a Fortigate even if there is no existing session.

```
config system settings
   set asymroute-icmp enable
   set asymroute6-imap enable
   end
```

When feature enabled:

- Allows ICMP or ICMPv6 reply traffic can pass through firewall when there is no session existing - asymmetric routing case.

When feature disabled:

- Prevents ICMP or ICMPv6 replies from passing through firewall when there is no session existing.

Policy names (246575 269948 293048)

In addition to the Policy ID #, there is now a Policy name field in the policy settings. On upgrading to 5.4, policy names will not be assigned to old policies but when configuring new policies, a unique name must be assigned to it. Every policy name must be unique for the current VDOM regardless of policy type.

In the GUI, the field for the policy name is the first field on the editing page.

In the CLI, the syntax for assigning the policy name is:

```
config firewall [policy|policy6]
   set name <policy_name>
   end
```

The feature can be turned on or off.

To turn it off in the CLI:

```
config system settings
   set gui-advance-policy[enable|disable]
   end
```

To turn it off in the GUI, the ability to enable or disable it in the GUI must be enabled in the CLI.It is disabled by default.The syntax is:

```
config system settings
   set gui-allow-unamed-policy [enable | disable]
   end
```

Once it has been enabled, the requirement for named passwords can be relaxed by going to **System > Feature Select**. **Allow Unamed Policies** can be found under **Additional Features**.

This setting is VDOM based so if you are running VDOMs you will have to enter the correct VDOM before entering the CLI commands or turning the feature on or off in the GUI.

Policy and route lookup (266996 222827)

The **Policy Lookup** button in the menu bar at the top of the IPv4 and IPv6 Policy pages is used to determine the policy that traffic with a particular set of parameters will use. Once the parameters are entered, the policy that the traffic will use is displayed.

The parameters are:

- Source Interface - select from drop down menu of available interfaces
- Protocol - select from a drop down menu of:
  - IP
  - TCP
  - UDP
  - SCTP
  - [ICMP|ICMPv6]
  - [ICMP|ICMPv6] ping request
  - [ICMP|ICMPv6] ping reply
- Source - Source IP address
- Source Port
- Destination - Destination IP address
- Protocol Number - *if Protocol = IP*
- Source Port - *if Protocol = TCP|UDP|SCTP*
- Destination Port - *if Protocol = TCP|UDP|SCTP*
- ICMP Type - *if Protocol = ICMPv6*
- ICMP Code - *if Protocol = ICMPv6*

Support NAT 64 CLAT (244986)

NAT64 CLAT traffic is now supported by the FortiGate. CLAT traffic comes from devices that use the SIIT translator that plays a part in affecting IPv6 - IPv4 NAT translation.

VIPs can contain FQDNs (268876)

Instead of mapping to an IP address VIP can use a Fully Qualified Domain Name. This has to be configured in the CLI and the FQDN must be an address object that is already configured in the address listing.

The syntax for using a FQDN is as follows:

```
config firewall vip
   edit <VIP id>
      set type fqdn
      set mapped-addr <FQDN address object>
      end
```

Access Control Lists (ACLs) (293399)

The access control list (ACL) feature allows you to deny IPv4 or IPv6 packets received at an NP6-accelerated interface based on source and destination address and service. If you add an access control policy to an interface, ACL checking is one of the first things that happens to the packet and checking is done by the NP6 processor. The result is very efficient protection that does not use CPU or memory resources.

In the GUI, the feature can be found at **Policy & Objects > IPv4 Access Control List Policy & Objects > IPv6 Access Control List.**

To add an IPv4 ACL through the CLI use the following syntax:

```
config firewall acl
   edit <acl Policy ID #>
      set status enable
      set interface <interface>
      set srcaddr <address object>
      set dstaddr <address object>
      set service <service object>
      end
   end
```

To add an IPv6 ACL through the CLI use the following syntax:

```
config firewall acl6
   edit <acl Policy ID #>
      set status enable
      set interface <interface>
      set srcaddr <address object>
      set dstaddr <address object>
      set service <service object>
      end
   end
```

GUI improvement for DoS Policy configuration (286905)

The user can now set the **Action**, whether **Pass** or **Block**, for all of the anomalies in a list at once when configuring a DoS policy.Just choose the desired option in the heading at the top of the column.

Expired Policy Object warnings (259338)

The Policy window indicates when a policy has become invalid due to its schedule parameters referring only to times in the past.

FortiGate VM

This chapter describes new FortiGate VM features added to FortiOS 5.4.

FortiGate VM cloud-init integration (300398)

Cloud-init is a set of pythons scripts and utilities commonly used for multi-distribution of VMs into cloud environments.

With cloud-init integration, when users launch a new instance of Fortigate VM, they can:

- Upload a license to a FGT-VM
- Provide initial management configuration, e.g. IP, default gateway, DNS
- Set port configuration mode (DHCP or static)
- Provision initial firewall policies

Cloud-init documentation can be found at https://cloudinit.readthedocs.io/en/latest/

Allow VM tools (VMWare platform) to set network settings for FortiGate VMS (292248)

Changes have been made to the firmware to mitigate the following issues:

- FGVM does not allow IP configuration during deployment.
- The use of multiple OVF files for different network adapter types is redundant.
- The sequence of interfaces is not kept in consistent with network adapters in VM settings.

These issues are corrected by the following changes:

- During deployment, the user will be prompted for an IP allocation policy (when using the new vApp OVF file). Static/DHCP can be selected for each port. Gateway can be configured for port1. Hostname, as well as primary/secondary DNS address, can be configured.
- During deployment, the user will be able to select either E1000 virtual network adapter or VMXNET3 ones (when using the new vApp OVF file).
- The new process keeps FGTVM's interface in the same sequence as the order shown in VM settings.
- There is an added CLI command "`diag vmware show-ovfenv`" to print out the whole OVF environment.

All additional features during deployment are only available when FGTVM is deployed through vCenter as a vApp.

- FGTVM interface sequence is determined with the following logic (and priority):
  - If OVF environment is available, the sequence present in the OVF environment will be used. (This is the preferred case. As the sequence can kept consistent with VM settings, regardless of whether adapters are removed/added, or mixed types of adapters are used.)
  - If the first network adapter is VMXNET3, FGTVM will use a dynamic mapping of interface, according to the total number of network adapters present. (This assumes all the network adapters are VMXNET3.)
  - If the above conditions do not qualify, FGTVM will use a static mapping of interface, which assumes every network adapter is E1000
- Even when a fixed IP allocation policy is selected during deployment, DHCP might be enabled on port1. This happens when the interface IP is set to 0.0.0.0 on port1. Unfortunately, OVF environment is unable to provide

which IP allocation policy has been selected. Rather, it is only able to give a set of IP/netmask on each of the interfaces.

- Configuration is applied AFTER IP allocation policy. This means, IP allocation policy works as default settings of interface, and is ignored when any existing configuration presents on a certain interface.

FortiKVM removed from most FortiGates (366859)

The FortiKVM feature that allowed a virtual instance of FortiGate on a FortiGate device is no longer part of FortiOS for most models. With few exceptions, this feature is being moved to FortiHypervisor, a specialised appliance with resources optimized for the purpose.

FortiKVM support added to select models (282335)

FortiKVM functionality is now available on the following models:

- FGT1500D
- FGT3700D
- FGT3700DX
- FGT3810D

Interface assignment CLI:

```
config system vm
   edit 0
      set name vm1
         config interface
            edit 1
               set name vnic1
               set device [physical | vlan | softswitch]
               mode [bridge | passthrough]
               end
            end
         end
```

[device]: can assign physical, VLAN, or softwitch type host interface to this attribute.

[mode]: this attribute is available only when device is assigned physical type interface, bridge mode means several vNIC can share this interface, when packet arrives, host will lookup vNIC by dst mac address, in passthrough mode, host will send all packets to the vNIC, only one vNIC can use the physical interface in passthrough mode.

FGT-VM VMX (v2) (306438)

FortiGate-VM VMX version 2 allows for automated deployment of virtual FortiGate instances running FortiOS 5.4.1 in a specific VMWare SDN environment. For more details read the Release Notes and Admin Guides for FortiGate-VM VMX.

FortiOS On-Demand (308130)

New VM platform to support a consumption based FOS VM pricing model.FortiOS On-Demand supports VMWare hypervisor, and Openstack KVM hypervisor platforms.

- These platforms have three interfaces only: mgmt, port1, and port2.
- port1 and port2 are used for metering, and is reported to a FortiManager via the updated process.
- The FortiManager is configured externally via Vapp for VMware or user-data in KVM.
- FortiGuard updates and webfiltering servers will initially point to the FortiManager.
- The FortiManager will authorize the FOSVM instance. If not authorized the vdom is disabled.

Changes to FG-VM00 Min/Max Values (246780,372030)

- The maximum memory virtual memory has changed from 1 to 1.5 GB.
- The maximum number of VDOMs has changed from 1 to 2.

Integrate VMtools Into FortiGate-VM for VMware (248842)

The following VMtools sub set of features has been integrated into the FortiGate-VM for VMWare images:

- Start
- Stop
- Reboot
- IP state in vCenter

VM License Check Time Extension (262494)

VM license check time has been extended to 30 days, with daily warning notifications and a counter.

FortiGate VM Single Root I/O Virtualization (SR-IOV) support (275432)

SR-IOV is a specification that allows a PCIe device to be treated as multiple separate PCIe devices.This feature will enable better performance with Intel based servers across multiple VM platforms, including Citrix and AWS. In fact, AWS has optimized some instance types to take advantage of this feature.

You can reset FortiGate VMs to factory defaults without deleting the VM license (280471)

New command , **`execute factoryreset keepvmlicense`**, resets FortiGate VMs to factory defaults without deleting the VM license.

Hardware acceleration

This chapter describes new authentication features added to FortiOS 5.4.

Offload Diffie-Hellman processing for 3072- and 4096-bit Diffie-Hellman values (308040)

Server load balancing supports 3072 and 4096 bit DH values. The command syntax is:

```
config firewall vip
   edit server-name
      set type server-load-balance
      set server-type https
      set ssl-dh-bits {768 | 1024 | 1536 | 2048 | 3072 | 4096}
```

FortiGate models with CP9 processors support 3072 and 4096 DH bit sizes in hardware. All FortiGate models up to and including those with CP8 processors only support offloading DH bit sizes up to 2048 so any sizes larger than that are done in software and thus are relatively resource intensive.

NP6 diagnose commands and get command changes (288738)

You can use the `get hardware npu np6` command to display information about the NP6 processors in your FortiGate and the sessions they are processing. This command contains a subset of the options available from the `diagnose npu np6` command. The command syntax is:

```
get hardware npu np6 {dce <np6-id> | ipsec-stats | port-list | session-stats <np6-id> |
    sse-stats <np6-id> | synproxy-stats}
```

`<np6-id>` identifies the NP6 processor. `0` is `np6_0`, `1` is `np6_1` and so on.

`dce` show NP6 non-zero sub-engine drop counters for the selected NP6.

`ipsec-stats` show overall NP6 IPsec offloading statistics.

`port-list` show the mapping between the FortiGate's physical ports and its NP6 processors.

`session-stats` show NP6 session offloading statistics counters for the selected NP6.

`sse-stats` show hardware session statistics counters.

`synproxy-stats` show overall NP6 synproxy statistics for TCP connections identified as being syn proxy DoS attacks.

NP6 session accounting enabled when traffic logging is enabled in a firewall policy (268426)

By default, on a FortiGate unit with NP6 processors, when you enable traffic logging in a firewall policy this also enables NP6 per-session accounting. If you disable traffic logging this also disables NP6 per-session accounting. This behavior can be changed using the following command:

```
config system np6
   edit np6_0
      set per-session-accounting {disable | all-enable | enable-by-log}
   end
```

By default, `per-session-accounting` is set to `enable-by-log`, which results in per-session accounting being turned on when you enable traffic logging in a policy. You can disable per-session accounting or set `all-enable` to enable per-session accounting whether or not traffic logging is enabled. Note that this configuration is set separately for each NP6 processor.

When offloaded sessions appear on the FortiView All Sessions console they include an icon identifying them as NP sessions:

Application	Bytes (Sent/Received)	Policy
TCP/443	29.16 kB	Local In
YouTube	NP 219.44 kB	my-policy
UDP/53	31.05 kB	Local In

You can hover over the NP icon to see some information about the offloaded sessions.

Determining why a session is not offloaded (245447)

You can use the `diagnose sys session list` command to get information about why a session has not been offloaded to an NP4 or NP6 processor.

If a session has not been offloaded the session information displayed by the command includes `no_ofld_reason` followed by information to help you determine the cause. To take a simple example, an HTTPS session connecting to the GUI could have a field similar to `no_ofld_reason: local`. This means the session is a local session that is not offloaded.

The `no_ofld_reason` field only appears if the session is not offloaded and includes information to help determine why the session is not offloaded. For example,

```
no_ofld_reason: redir-to-av redir-to-ips non-npu-intf
```

Indicates that the session is not offloaded because it was redirected to virus scanning (`redir-to-av`), IPS (`redir-to-ips`), and so on.

IPsec pass-through traffic is now offloaded to NP6 processors (253221)

IPsec traffic that passes through a FortiGate without being unencrypted is now be offloaded to NP6 processors.

Disabling offloading IPsec Diffie-Hellman key exchange (269555)

You can use the following command to disable using ASIC offloading to accelerate IPsec Diffie-Hellman key exchange for IPsec ESP traffic. By default hardware offloading is used. For debugging purposes or other reasons you may want this function to be processed by software.

Use the following command to disable using ASIC offloading for IPsec Diffie Hellman key exchange:

```
config system global
   set ipsec-asic-offload disable
end
```

FortiGate-3700DX TP2 processors support GTP offloading (294212)

The FortiGate-3700DX contains two TP2 processors that provide GTP offloading. GTPu traffic is forwarded from NP6 processors to TP2 processors. The TP2 processors filter the encapsulated traffic and send the approved GTPu traffic back to the NP6.

Preventing packet ordering problems with NP4 and NP6 FortiGates under heavy load (365497)

In some cases when FortiGate units with NP4 or NP6 processors are under heavy load the packets used in the TCP 3-way handshake of some sessions may be transmitted by the FortiGate in the wrong order resulting in the TCP sessions failing.

If you notice TCP sessions failing when a FortiGate with NP4 or NP6 processors is very busy you can enable `delay-tcp-npu-session` in the firewall policy receiving the traffic. This option resolves the problem by delaying the session to make sure that there is time for all of the handshake packets to reach the destination before the session begins transmitting data.

```
config firewall policy
   set delay-tcp-npu-session enable
end
```

High Availability

This chapter describes new high availability features added to FortiOS 5.4.

HA diagnose checksum command changes (259710)

The following diagnose commands changed:

- `diagnose sys ha showcsum` --> `diagnose sys ha checksum show`
- `diagnose sys ha csum-recalculate` --> `diagnose sys ha checksum recalculate`
- `diagnose sys ha cached-csum` --> `diagnose sys ha checksum cached`
- `diagnose sys ha cluster-csum` --> `diagnose sys ha checksum cluster`

FGCP supports BFD enabled BGP graceful restart after an HA failover (255574)

If an HA cluster is part of a Border Gateway Protocol (BGP) bidirectional forwarding detection (BFD) configuration where both the cluster and the BGP static neighbor are configured for graceful restart, after an HA failover BGP enters graceful restart mode and both the cluster and the BGP neighbor keep their BGP routes.

To support HA and BFD enabled BGP graceful:

- From the cluster, you can add a BFD enabled BGP neighbor as a static BFD neighbor using the `config router bfd` command. Set the BGP auto-start timer to 5 seconds so that after an HA failover BGP on the new primary unit waits for 5 seconds before connect to its BFD neighbors, and then registers BFD requests after establishing the connections. With static BFD neighbors, BFD requests and sessions can be created as soon as possible after the failover. The command `get router info bfd requests` shows the BFD peer requests.
- The BFD session created for a static BFD neighbor/peer request initializes its state as INIT instead of DOWN and its detection time as `bfd-required-min-rx * bfd-detect-mult` msecs.
- When a BFD control packet with a nonzero Your Discriminator (`your_discr`) value is received, if no session can be found to match the `your_discr`, instead of discarding the packet, other fields in the packet, such as addressing information, are used to choose one session that was just initialized, with zero as its remote discriminator.
- When a BFD session in the UP state receives a control packet with zero as Your Discriminator and DOWN as State, the session changes its state to DOWN but will not notify this DOWN event to BGP and/or other registered clients.

FRUP is not supported by FortiOS 5.4 (295198)

With the changes to switch mode, FRUP is no longer available on the FortiGate-100D.

VOIP application control sessions are no longer blocked after an HA failover (273544)

After an HA failover, VoIP sessions that are being scanned by application control will now continue with only a minor interruption, if any. To support this feature, IPS UDP expectation tables are now synchronized between cluster units.

Firewall local-in policies are supported for the dedicated HA management interface (276779 246574)

To add local in polices for the dedicated management interface, enable `ha-mgmt-inft-only` and set `intf` to `any`. Enabling `ha-mgmt-intf-only` means the local-in policy applies only to the VDOM that contains the dedicated HA management interface.

```
config firewall local-in-policy
   edit 0
      set ha-mgmt-intf-only enable
      set intf any
      etc...
   end
```

HA heartbeat traffic set to the same priority level as data traffic (276665)

Local out traffic, including HA heartbeat traffic, is now set to high priority to make sure it is processed at the same priority level as data traffic. This change has been made because HA heartbeat traffic can be processed by NP6 processors that are also processing data traffic. When HA heartbeat traffic was set to a lower priority it may have be delayed or dropped by very busy NP6 processors resulting in HA failovers.

FGSP CLI command name changed (262340)

The FortiOS 5.2 command `config system session-sync` has been changed in FortiOS 5.4 to `config system cluster-sync`. Otherwise the command syntax is the same and the `config system ha` commands used for FGSP settings have not changed.

FGSP now supports synchronizing IPsec sessions (262340)

The FGSP now synchronizes IPsec tunnels between FortiGates in an FGSP configuration. IPsec tunnel synchronization synchronizes keys and other run time data between the FortiGates in an FGSP configuration. No additional configuration is required to synchronize IPsec sessions. Also you cannot disable IPsec tunnel synchronization.

The FGSP synchronizes IPsec keys and other runtime data but not actual tunnel sessions. This means that if one of the cluster units goes down the cluster unit that is still operating can quickly get IPsec tunnels re-established without re-negotiating them but all existing tunnel sessions on the failed FortiGate have to be restarted on the still operating FortiGate.

IPsec tunnel sync only supports dialup IPsec. The interfaces on both FortiGates that are tunnel endpoints must have the same IP addresses and external routers must be configured to load balance IPsec tunnel sessions to the FortiGates in the cluster.

Monitoring VLAN interfaces (220773)

When operating in HA mode and if you have added VLAN interfaces to the FortiGates in the cluster, you can use the following command to monitor all VLAN interfaces and send a message if one of the VLAN interfaces is found to be down.

```
config system ha-monitor
   set monitor-vlan enable/disable
```

```
    set vlan-hb-interval <interval_seconds>
    set vlan-hb-lost-threshold <vlan-lost-heartbeat-threshold>
end
```

Once configured, this feature works by verifying that the primary unit can connect to the subordinate unit over each VLAN. This verifies that the switch that the VLAN interfaces are connected to is configured correctly for each VLAN. If the primary unit cannot connect to the subordinate unit over one of the configured VLANs the primary unit writes a link monitor log message indicating that the named VLAN went down (log message id 20099).

Improvements to the get system ha status command output (259416)

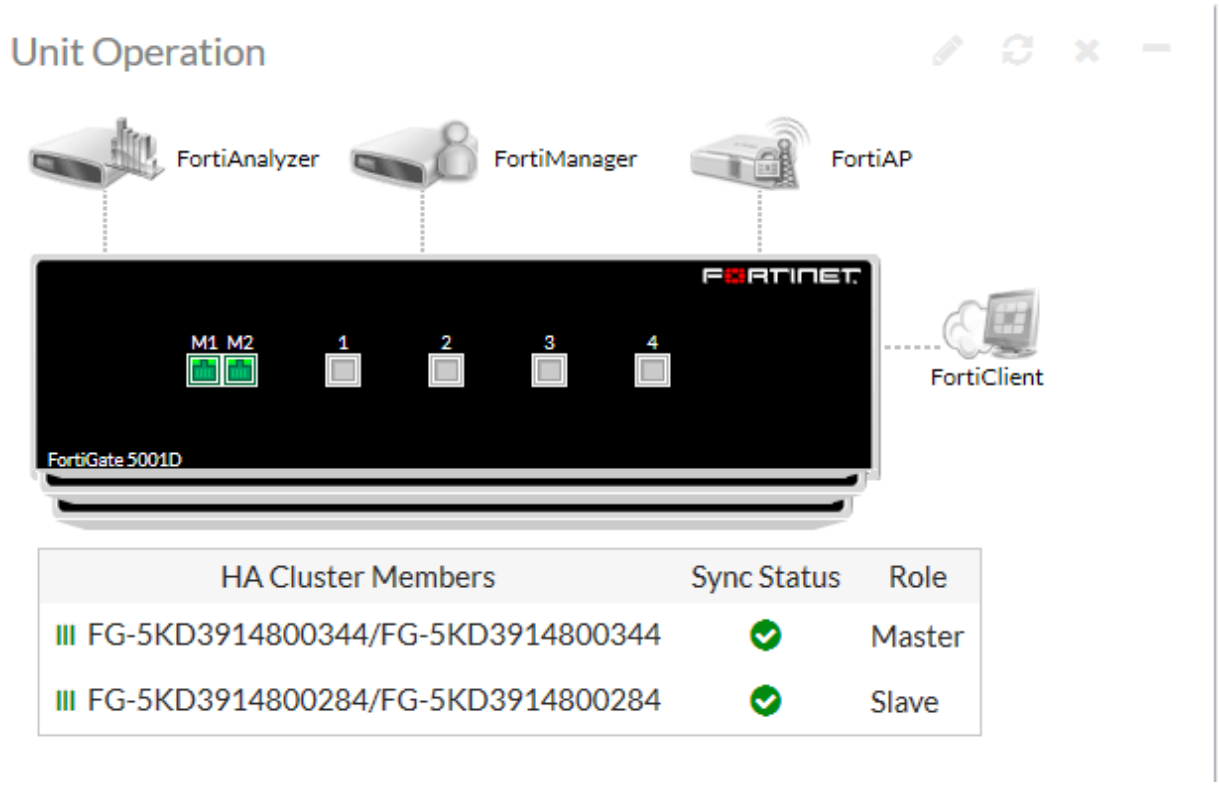
The get system ha status command now displays more information about cluster status including HA health status, cluster uptime, how the primary unit was selected and when this happened, override status, HA heartbeat interface activity, and CPU and memory usage for each cluster unit.

FortiGate HA cluster support for managed switches (276488 266084)

Added the capability to support managed switches from a FortiGate HA cluster. If a standby FortiGate becomes active, it automatically establishes connectivity with the managed switches.

HA cluster health displayed on the Unit Operation dashboard widget (260547)

The Unit Operation dashboard widget now includes the serial number and hostname of all of the FortiGate units in the cluster as well as an indication of the sync status of each cluster member.



IPsec VPN

This chapter describes new IPsec VPN features added to FortiOS 5.4.

Added warning message in IPsec VPN wizard if users selects ANY for peer ID (357043)

If users change the **peertype** setting back to **any**, either via CLI or GUI, they receive a warning that clearly informs them that using a setting of **any** will allow remote connections generated by any CA trusted by this FortiGate to be established.

- Warning icon shows up in IPsec tunnel page when setting **peertype** to **any** in VPN tunnel.
- Warning message shows up in IPsec tunnel editing page when setting **peertype** to **any** in VPN tunnel.
- In the VPN wizard configuration page, option **peer certificate CA** is added which is used to create the related peer user through VPN wizard.
- **Peertype** is set to **peer certificate** by default in GUI when setting **authmethod** to **signature** for custom IPsec tunnel.

IKEv1 Quick Crash Detection (304612)

Based on the IKEv2 quick crash detection (QCD) feature in Mantis 298970, which is already in the new features list for FortiOS 5.4 below.

There is no RFC for this feature. It is implemented using a new IKE vendor ID, "Fortinet Quick Crash Detection", and so both endpoints must be FortiGate devices. The QCD token is sent in the Phase 1 exchange and must be encrypted, so this is only implemented for IKEv1 in Main mode (Aggressive mode is not supported as there is no available AUTH message in which to include the token).

Otherwise, the feature works the same as in IKEv2 (RFC 6290).

IKE mode-cfg IPv4/IPv6 dual stack support (303550)

The previous IKE CLI uses the `mode-cfg-ip-version` option to specify whether `mode-cfg` should assign an IPv4 or IPv6 address, but this is not ideal for customers that require dual stack support.

As a solution in FortiOS 5.4.1, the `phase1 mode-cfg-ip-version` option was removed. The option was not necessary because the IP version can be determined by the selector type (`dst-addr-type`) of the configured Phase 2 tunnel(s). If the FortiGate client config contains Phase 2 tunnels for both IPv4 and IPv6, then the FortiGate client will request IPv4 and IPv6 addresses during `mode-cfg`.

Additionally, the FGT server can now be configured to reply with either or both IPv4 and IPv6, as per the client's `mode-cfg` request.

Security improvements to the default IPsec VPN signature and peer type configuration (304894 307500 307490 355149)

New features have been introduced to make certification and implementation in IPsec VPN more secure by default. Users can now create PKI certificates in-line in the VPN editor.

In short:

- Reimplemented PKI dialogs such that changes to enforce attributes are done in new frameworks
- Changed default templates for VPN wizard to enforce `peertype=any` so that wizard tunnels can be created
- Will now default to PKI string when creating signature VPN via VPN edit

Remote IP address change detection (209553)

This feature changes the way IPsec SAs are tracked in the kernel in order to detect external IP address changes in the tunnel.

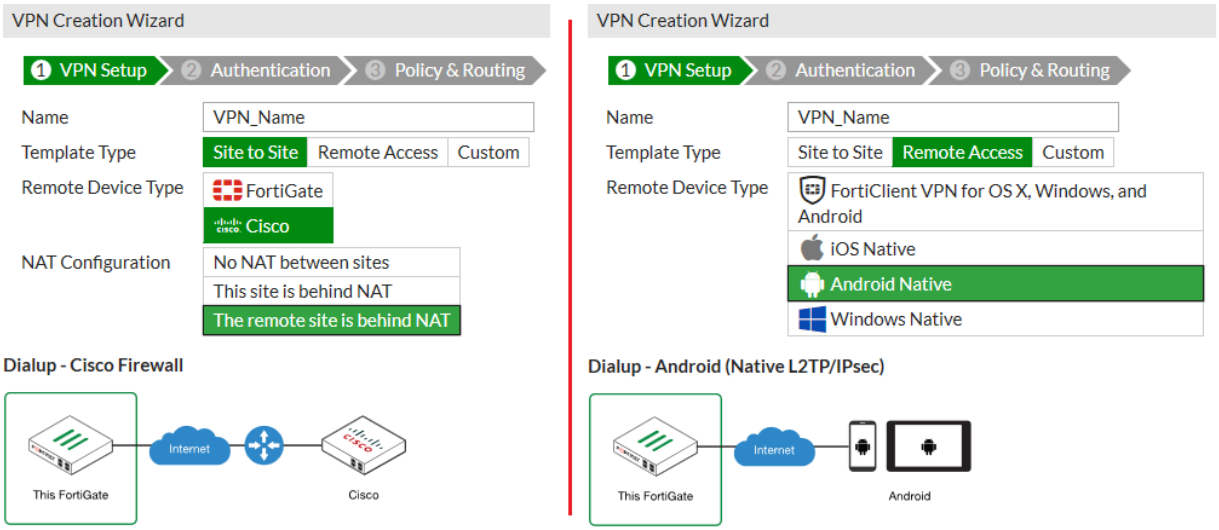
Previously, SAs were stored when keyed off of the remote IP address. Now, SAs are stored in a hash table when keyed off the IPsec SA SPI value (which is actually more RFC compliant). This enables the FortiGate, for each inbound ESP packet received, to immediately look up the SA and compare the stored IP address against the one in the incoming packet. If the incoming and stored IP addresses differ, an IP address change can be made in the kernel SA, and an update event can be triggered for IKE.

IKE/IPsec Extended Sequence Number (ESN) support (255144)

This feature implements negotiation of 64-bit Extended Sequence numbers as described in RFC 4303, RFC 4304 as an addition to IKEv1, and RFC 5996 for IKEv2.

Updates and enhancements to the IPsec VPN wizard (222339 290377 287021 289251)

The IPsec VPN wizard has been simplified to more clearly identify tunnel template types, remote device types, and NAT configuration requirements. Example topological diagrams are now also included.



New **Dialup - FortiGate** and **Dialup - Windows (Native L2TP/IPsec)** tunnel template options.

Cisco compatible keep-alive support for GRE (261595)

The FortiGate can now send a GRE keep-alive response to a Cisco device to detect a GRE tunnel. If it fails, it will remove any routes over the GRE interface.

Syntax

```
config system gre-tunnel
   edit <id>
      set keepalive-interval <value: 0-32767>
      set keepalive-failtimes <value: 1-255>
   next
end
```

Repeated Authentication in Internet Key Exchange (IKEv2) Protocol (282025)

This feature provides the option to control whether a device requires its peer to re-authenticate or whether re-key is sufficient. It does not influence the re-authentication or re-key behavior of the device itself, which is controlled by the peer (with the default being to re-key).

This solution is in response to RFC 4478. As described by the IETF, "the purpose of this is to limit the time that security associations (SAs) can be used by a third party who has gained control of the IPsec peer".

Syntax

```
config vpn ipsec phase1-interface
   edit p1
      set reauth [enable | disable]
   next
end
```

Improvements to IPsec VPN in ADVPN hub-and-spoke (275322)

IPsec VPN traffic is now allowed through a tunnel between an ADVPN hub-and-spoke

```
config vpn ipsec phase1-interface
   edit "int-fgtb"
      ...
      set auto-discovery-sender [enable | disable]
      set auto-discovery-receiver [enable | disable]
      set auto-discovery-forwarder [enable | disable]
      ...
   next
end
config vpn ipsec phase2-interface
   edit "int-fgtb"
      ...
      set auto-discovery-sender phase1 [enable | disable]
      ...
   next
end
```

ADVPN support for NAT device (299798)

The ADVPN feature has been extended so that it allows ADVPN shortcuts to be negotiated as long as one of the devices is not behind NAT.

The on-the-wire format of the ADVPN messages was changed so that they use TLV encoding. Since the on-the-wire format has changed this is not compatible with any previous ADVPN builds.

AES-GCM support (281822)

AES-GCM (128 | 256) AEAD has been added, as specified in **RFC 4106**:

```
config vpn ipsec phase1-interface
   edit "tofgta"
      ...
      set suite-b disable | suite-b-gcm-128 | suite-b-gcm-256
      ...
   next
end
config vpn ipsec phase2-interface
   edit "tofgta"
      set phase1name "tofgta"
      set proposal aes128gcm aes256gcm
      ...
   next
end
```

IPsec tunnel idle timer (244180)

Add a command to define an idle timer for IPsec tunnels when no traffic has passed through the tunnel for the configured idle-timeout value, the IPsec tunnel will be flushed.

```
config vpn ipsec phase1-interface
   edit p1
      set idle-timeout enable/disable
      set idle-timeoutinterval <integer> //IPsec tunnel idle timeout in minutes (10 - 43200).
   end
end
```

SAs negotiation improvement (245872)

The IPsec SA connect message generated is used to install dynamic selectors. These selectors can now be installed via the auto-negotiate mechanism. When phase 2 has auto-negotiate enabled, and phase 1 has mesh-selector-type set to **subnet**, a new dynamic selector will be installed for each combination of source and destination subnets. Each dynamic selector will inherit the auto-negotiate option from the template selector and begin SA negotiation. Phase 2 selector sources from dial-up clients will all establish SAs without traffic being initiated from the client subnets to the hub.

Add VXLAN over IPsec (265556)

Packets with VXLAN header are encapsulated within IPsec tunnel mode. New attributes in IPsec phase1 settings have been added.

```
config vpn ipsec phase1-interface/phase1
   edit ipsec
```

```
        set interface <name>
        set encapsulation vxlan/gre (new)
        set encapsulation-address ike/ipv4/ipv6 (New)
        set encap-local-gw4 xxx.xxx.xxx.xxx (New)
        set encap-remote-gw xxx.xxx.xxx.xxx (New)
    next
end
```

Ability to enable/disable IPsec ASIC-offloading (269555)

Much like NPU-offload in IKE phase1 configuration, this feature enables/disables the usage of ASIC hardware for IPsec Diffie-Hellman key exchange and IPsec ESP traffic. Currently by default hardware offloading is used. For debugging purposes, sometimes we want all the traffic to be processed by software.

```
config sys global
   set ipsec-asic-offload [enable | disable]
end
```

Added an option to force IPsec to use NAT Traversal (275010)

Added a new option for NAT. If NAT is set to Forced, then the FGT will use a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC.

Add a feature to support IKEv2 Session Resumption described in RFC 5723 (289914)

If a gateway loses connectivity to the network, clients can attempt to re-establish the lost session by presenting the ticket to the gateway. As a result, sessions can be resumed much faster, as DH exchange that is necessary to establish a brand new connection is skipped. This feature implements "ticket-by-value", whereby all information necessary to restore the state of a particular IKE SA is stored in the ticket and sent to the client.

Added support for IKEv2 Quick Crash Detection (298970)

A new feature has been added to support IKEv2 Quick Crash Detection as described in RFC 6290.

RFC 6290 describes a method in which an IKE peer can quickly detect that the gateway peer that it has and established IKE session with, has rebooted, crashed, or otherwise lost IKE state. When the gateway receives IKE messages or ESP packets with unknown IKE or IPsec SPIs, the IKEv2 protocol allows the gateway to send the peer an unprotected IKE message containing INVALID_IKE_SPI or INVALID_SPI notification payloads.

RFC 6290 introduces the concept of a QCD token, which is generated from the IKE SPIs and a private QCD secret, and exchanged between peers during the protected IKE AUTH exchange.

CLI Syntax

```
config system settings
   set ike-quick-crash-detect [enable | disable]
end
```

- If updating to FortiOS 5.4.1, see above (304612).

Removed support for auto-IPsec (300893)

IPsec auto-VPN support (auto-IPsec) has been removed. This feature was added in FortiOS 5.0 prior to any usable VPN creation support on the GUI. As of 5.2, and now in 5.4, the wizard solves many of the problems introduced by the auto-IPsec feature, and so auto-IPsec has been deprecated.

Improved scalability for IPsec DPD (292500)

On a dial-up server, if a multitude of VPN connections are idle, the increased DPD exchange could negatively impact the performance/load of the daemon. For this reason, an option has been added to send DPD passively in a mode called "on-demand".

```
config vpn ipsec phase1-interface
   edit <value>
      set dpd [disable | on-idle | on-demand]
   next
end
```

Notes

- When there is no traffic and the last DPD-ACK had been received, IKE will not send DPDs periodically.
- IKE will only send out DPDs if there are outgoing packets to send but no inbound packets had since been received.

Syntax

The `set dpd enable` command has changed to `set dpd on-idle` (to trigger DPD when IPsec is idle). Set DPD to `on-demand` to trigger DPD when IPsec traffic is sent but no reply is received from the peer.

```
configure vpn ipsec phase1-interface
   edit <value>
      set dpd [on-idle|on-demand]
   next
end
```

IPv6

DHCPv6 server is configurable in delegated mode (295007)

Downstream IPv6 interfaces can receive address assignments on delegated subnets from a DHCP server that serves an upstream interface.

DHCPv6-PD configuration

Enable DHCPv6 Prefix Delegation on upstream interface (port10):

```
config system interface
   edit "port10"
     config ipv6
       set dhcp6-prefix-delegation enable
     end
end
```

Assign delegated prefix on downstream interface (port1). Optionally, specific delegated prefixes can be specified:

```
config system interface
   edit "port1"
     config ipv6
       set ip6-mode delegated
       set ip6-upstream-interface "port10"
       set ip6-subnet ::1:0:0:0:1/64
       set ip6-send-adv enable
       config ipv6-delegated-prefix-list
         edit 1
           set upstream-interface "port10"
           set autonomous-flag enable
           set onlink-flag enable
           set subnet 0:0:0:100::/64
         end
     end
   end
```

DHCPv6 Server configuration

Configuring a server that uses delegated prefix and DNS from upstream:

```
config system dhcp6 server
   edit 1
     set dns-service delegated
     set interface "wan2"
     set upstream-interface "wan1"
     set ip-mode delegated
     set subnet 0:0:0:102::/64
   end
```

FortiGate can connect to FortiAnalyzer using IPv6 addresses (245620)

When configuring your FortiGate to send logs to a FortiAnalyzer you can specify an IPv4 or an IPv6 address.

IPv6 neighbor discovery limits changes(248076)

You can use the following command to configure the maximum number of IPv6 neighbors that can be discovered by the IPv6 Neighbor Discovery Protocol (NDP) and added to the IPv6 neighbor database.

```
config system global
   set ndp-max-entry <integer>
end
```

The number of entries can be in the range 65,536 to 2,147,483,647. The default value of 0 means 65,536 entries.

Support IPv6 blackhole routing (220101)

Similar to IPv4 blackhole routing, IPv6 blackhole routing is now supported. Use the following command to enable IPv6 blackhole routing:

```
config router static6
   edit 1
      set blackhole enable/disable
   next
end
```

TFTP session helper for IPv6 (263127)

TFTP is supported over nat66 and nat46.

FTP, PPTP and RTSP session helper enhancements for IPv6 (244986)

The FTP, PPTP and RTSP session helpers support NAT-64 customer-side translator (CLAT) sessions.

Central Management ratings and update servers can use IPv6 addresses (297144)

You can configure servers for Central Management using either IPv4 or IPv6 addresses. The `addr-type` field sets the address type. The address is entered in the `server-address` or `server-address6` field as appropriate.

```
config system central-management
   set type fortimanager
   set fmg "2000:172:16:200::207"
   set vdom "vdom1"
   config server-list
      edit 1
         set server-type rating update
         set addr-type ipv6
         set server-address6 2000:172:16:200::207
      end
```

```
    end
```

Allow asymmetric routing for ICMP (258734)

Where network topology requires asymmetric routing for ICMP traffic, you can configure the FortiGate to permit the asymmetric ICMP traffic. This is done in the CLI. There are separate fields for IPv4 and IPv6 versions of ICMP.

```
config system settings
   set asymroute-icmp enable
   set asymroute-icmp6 enable
end
```

Load balancing

This chapter describes new load balancing features added to FortiOS 5.4.

Separate virtual-server client and server TLS version and cipher configuration (308040)

In previous versions of FortiOS you can configure minimum and maximum SSL/TLS versions that a virtual server will accept. Those versions primarily applied to the client to FortiGate connection; but, they are also applied to the FortiGate to server connection. In some cases you may want to use different versions of SSL or TLS on the client to FortiGate connection than on the FortiGate to server connection. For example, you may want to use the FortiGate to protect a legacy SSL 3.0 or TLS 1.0 server while making sure that client to FortiGate connections must always use the higher level of protection offered by TLS 1.1 or greater.

Similarly in previous versions of FortiOS you could control the cypher suites that can be used by the FortiGate to negotiate with the client and with the server. But you could only configure the same configuration for both client and server connections. Also, in some cases you might want to protect a server that only has weak ciphers (for example, DES or RC4) while making sure that all connections between the FortiGate and the client use a strong cipher for better protection.

The following new options are available when configuring server load balancing for HTTPS sessions configured with the following command:

```
config firewall vip
   edit server-name
      set type server-load-balance
      set server-type https
      set ssl-mode full
      ...
```

Different SSL/TLS versions for server and client connections

New `ssl-server-min-version` and `ssl-server-max-version` configuration options allow the minimum and maximum SSL/TLS versions for the client to FortiGate connection to be independent of the FortiGate to server configuration. By default these options are both set to `client` and the configured `ssl-min-version` and `ssl-max-version` settings are applied to both the client and the server connection.

You can change the `ssl-server-min-version` and `ssl-server-max-version` to apply different options to the server connection. The `ssl-min-version` and `ssl-max-version` settings are still applied to the client connection. If you set the `ssl-server-min-version` and `ssl-server-max-version` to an explicit version then both must be set to an explicit version.

The `ssl-server-min-version` and `ssl-server-max-version` options allow you to specify the minimum and maximum SSL/TLS versions the FortiGate will offer to the server (in the record header of the ClientHello) when performing full mode SSL offloading and thus the minimum and maximum SSL/TLS versions the FortiGate accepts from the server (in a ServerHello). If the server responds with a version in its ServerHello that is lower than `ssl-server-min-version` or higher than the `ssl-server-max-version` then the FortiGate terminates the connection.

Command syntax is:

```
config firewall vip
   edit server-name
```

```
        set type server-load-balance
        set server-type https
        set ssl-mode full
        set ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}
        set ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}
        set ssl-server-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 | client}
        set ssl-server-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 | client}
```

Different cipher choices for server and client connections

New `ssl-server-algorithm` configuration option allows the cipher choice for the FortiGate to server connection to be independent of the client to FortiGate connection. By default, `ssl-server-algorithm` is set to `client` and the configured `ssl-algorithm` setting is applied to both the client and the server connection.

You can change the `ssl-server-algorithm` to apply different options to the server connection. The `ssl-algorithm` setting is still applied to the client connection.

The following `ssl-server-algorithm` options are available:

- `high`, offer AES or 3DES cypher suites in the ServerHello
- `medium`, use AES, 3DES, or RC4 cypher suites in the ServerHello
- `low`, use AES, 3DES, RC4, or DES cypher suites in the ServerHello
- `custom`, specifiy custom cypher suites using the `config ssl-server-cipher-suites` and offer these custom cypher suites in the ServerHello.
- `client`, offer the cypher suites in the ServerHello that are offered in the ClientHello.

Command syntax is:

```
config firewall vip
   edit server-name
      set type server-load-balance
      set server-type https
      set ssl-mode full
      set ssl-algorithm {high | medium | low | custom}
      set ssl-server-algorithm {high | medium | low | custom | client}
```

If you set ssl-server-algorithm to custom, the syntax is:

```
config firewall vip
   edit server-name
      set type server-load-balance
      set server-type https
      set ssl-mode full
      set ssl-server-algorithm custom
         config ssl-server-cipher-suites
            edit 10
               set cipher <cipher-suite>
               set versions {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}
            next
            edit 20
               set cipher <cipher-suite>
               set versions {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}
            end
         end
```

Protection from downgrade attacks

The new `ssl-client-fallback` option, when enabled (the default configuration), performs downgrade attack prevention (RFC 7507).

Command syntax is:

```
config firewall vip
   edit server-name
      set type server-load-balance
      set server-type https
      set ssl-client-fallback {disable | enable}
```

Allow 3072- and 4096-bit Diffie-Hellman values

New settings added to the `ssl-dh-bits` option to allow 3072 and 4096 bit DH values.

Command syntax is:

```
config firewall vip
   edit server-name
      set type server-load-balance
      set server-type https
      set ssl-dh-bits {768 | 1024 | 1536 | 2048 | 3072 | 4096}
```

The reason for adding these larger sizes is that the previous largest value of 2048 only provides the equivalent of a symmetric cipher in the range of 112 - 128 bits. This means that if AES 256 is used then the weakest point is the DH of 2048 and at least a value of 3072 should be use if the goal is to have 256 bits of security.

FortiGate models with CP9 processors support 3072 and 4096 DH bit sizes in hardware. All FortiGate models up to and including those with CP8 processors only support offloading DH bit sizes up to 2048 so any sizes larger than that are done in software and thus are relatively resource intensive.

ChaCha20 and Poly1305 cipher suites added for SSL load balancing (264785)

FortiOS 5.4 adds support for ChaCha20 and Poly1305 for SSL load balancing (see RFC 7539 for information about ChaCha20 and Poly1305). You can use the following command to view the complete list of supported cipher suites:

```
config firewall vip
   edit <vip-name>
      set type server-load-balance
      set server-type https
      set ssl-algorithm custom
         config ssl-cipher-suites
            edit 0
            set cipher ?
```

In most configurations the matching cipher suite is automatically selected.

All of these cipher suites are available to all of FortiOS's implementations of SSL but the complete list of supported cipher suites is only viewable using the above command.

You can also use the above command to limit the set of cipher suites that are available for a given SSL offloading configuration. For example, use the following command to limit an SSL load balancing configuration to use the three cipher suites that support ChaCha20 and Poly1305:

```
config firewall vip
   edit <vip-name>
      set type server-load-balance
      set server-type https
      set ssl-algorithm custom
         config ssl-cipher-suites
            edit 1
            set cipher TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256
            next
            edit 2
            set cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256
            next
            edit 3
            set cipher TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256
            end
         end
```

TLS 1.2 support for SSL offloading (241817)

You can use the following command to configure SSL offloading to support TLS 1.2:

```
config firewall vip
   edit <name>
      set type server-load-balance
      set server-type https
      set ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}
      set ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}
      ...
```

The default `ssl-min-version` is `tls-1.0` and the default `ssl-max-version` is `tls-1.2`.

The following AES-GCM TLS 1.2-only cipher suites have also been added. These cipher suites are not supported by the CPx or NPx processors so if you select one of these, all processing is done without hardware acceleration.

> TLS 1.2 support does not require setting `ssl-algorithm` to `custom` and configuring a custom cipher suite.

```
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
TLS-RSA-WITH-AES-128-GCM-SHA256
TLS-RSA-WITH-AES-256-GCM-SHA384
```

You can use the following command to select one of these cipher suites:

```
config firewall vip
   edit <name>
      set type server-load-balance
```

```
set server-type https
set ssl-max-version tls-1.2
set ssl-algorithm custom
   config ssl-cipher-suites
      edit 100
         set cipher TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
         ...
```

Logging and Reporting

This chapter describes new logging and reporting features added to FortiOS 5.4.

A new error log message is recorded when the Antispam engine request does not get a response from FortiGuard (265255)

Error code is '*sp_ftgd_error*'.

New Report database construction (280398 267019)

This will improve performance with reports and FortiView without requiring any configuration changes.

Communication between FortiGate and FortiAnalyzer supports IPv6 addresses (245620)

When configuring your FortiGate to send logs to a FortiAnalyzer you can specify an IPv4 or an IPv6 address.

Context menu on Log & Report > Forward Traffic has been updated (293188)

Now includes Policy Table and Device Quarantine controls.

Filtering allows control of the log messages sent to each log device (262061)

This includes disk log, memory log, FortiAnalyzer and syslog servers and allows inclusion/exclusion based on type, severity, and log ID.

Use the following CLI command:

```
config log <device> filter
   set filter <new-filter-settings>
   set filter-type <include | exclude>
end
```

Log messages in plain text LZ4 compressed format (271477 264704)

Log messages are stored on disk and transmitted to FortiAnalyzer as plain text in LZ4 compressed format. This change improves performance and reduces disk log size and reduces log transmission time and bandwidth usage.

Action and Security Action fields are improved (282691)

Action and Security Action fields in logs more clearly distinguishing between different uses of Action. Examples include traffic blocking by policy versus traffic blocking by security profile, or different result messages of Actions such as initiating session.

Log disk is full Event logs are deleted last (251467)

This feature should improve troubleshooting and diagnostics.

Send log messages to up to four syslog servers (279637)

You can use the CLI command `config log {syslogd | syslogd2 | syslogd3 | syslogd4}` to configure up to four remote syslog servers.

Changes to SNMP MIBs add the capability of logging dynamic routing activity (168927)

Examples include sending OSPF routing events or changes to a syslog server or FortiAnalyzer or changes in neighborhood status.

The syntax in the CLI for enabling the feature on BGP, OSPF and OSPF for IPv6 is as follows:

```
config router bgp
   set log-neighbour-changes [enable | disable]
   end

config router ospf
   set log-neighbour-changes [enable | disable]
   end

config router ospf6
   set log-neighbour-changes [enable | disable]
   end
```

Improve dynamic routing event logging (231511)

Major dynamic routing events such as neighbor down/up for BGP and OSPF are logged, without having to evoke debugging commands.

Adding option for VDOM logs through management VDOM (232284)

FortiOS supports the definition of per VDOM FortiAnalyzers. However it is required that each VDOM logs independently to its FortiAnalyzer server.

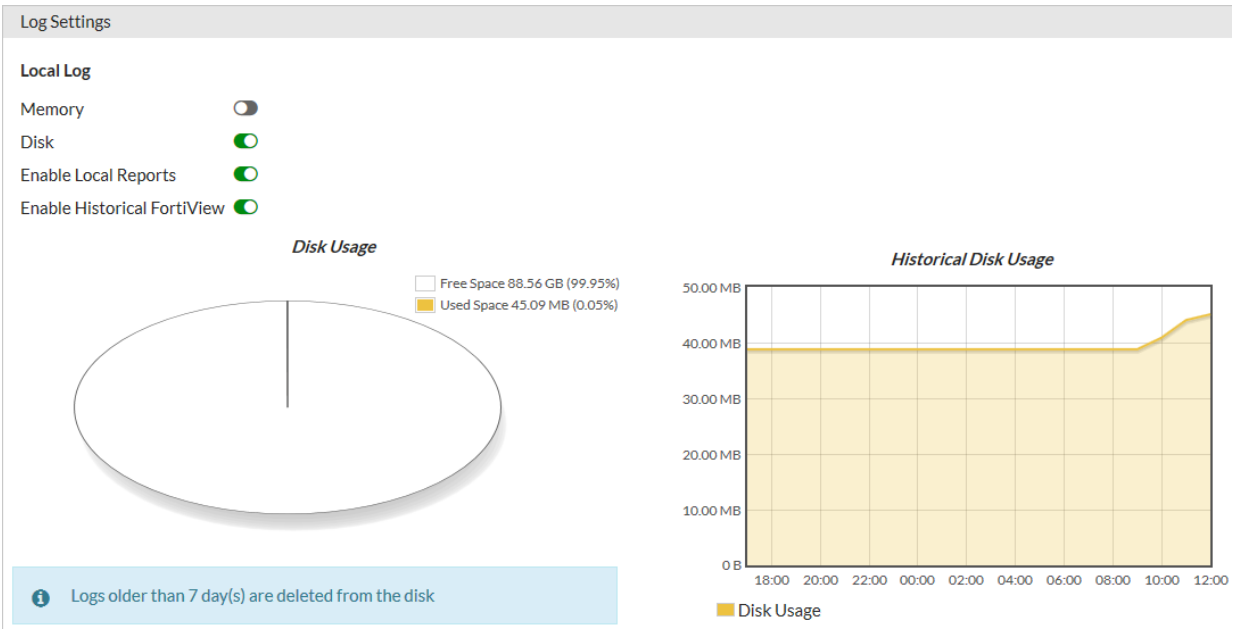
A new option, `use-management-vdom`, has been added to the CLI.

```
config vdom
   edit xxx
      config log fortianalyzer override-setting
         set use-management-vdom enable/disable
      end
   end
```

If this option is enabled, source-ip will become hidden and when FortiGate sends logs to FortiAnalyzer, it uses management vdom ip setting as source ip. Also if IPsec is enabled, the tunnel is created in management vdom and source ip belongs to management vdom.

The Log Settings GUI page displays information about current log storage (271318)

The Log Settings GUI page (Log & Report > Log Settings) displays information about current log storage including the amount of space available on the selected storage location and so on.



Log backup and restore tools (265285)

Local disk logs can now be backed up and restored, using new CLI commands.

```
exec log backup <filename>
exec log restore <filename>
```

Restoring logs will wipe the current log and report content off the disk.

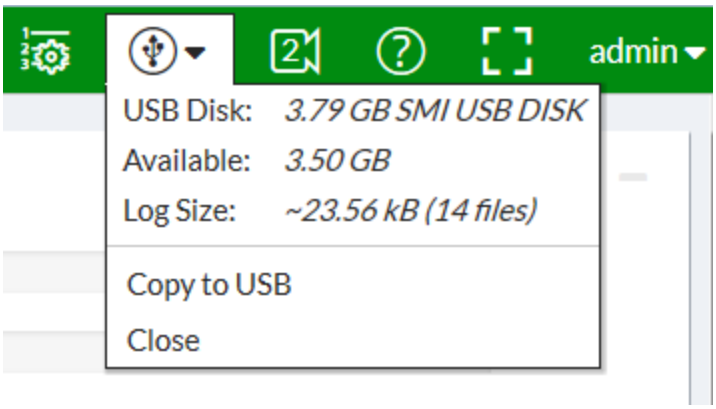
IPS logging optimization (254954)

The handling of IPS logs has been improved. No changes needed, just increased performance on the backend.

Export log messages to USB drive (258913 267501)

Logs can now be exported to a USB storage device, as Lz4 compressed files, from both CLI and GUI.

When you insert a USB drive into the FortiGate's USB port the USB menu appears on the GUI. The menu shows the amount of storage on the USB disk and the log file size and includes a **Copy to USB** option that you can use to copy the log file to the USB drive.



From the CLI you can use the following command to export all log messages stored in the FortiGate log disk to a USB drive:

```
execute backup disk alllogs usb
```

You can also use the following command to backup just traffic logs to a USB drive:

```
execute backup disk log usb traffic
```

Disable performance status logging by default (253700)

Performance statistic logging is now disabled by default. It can be re-enabled in CLI, to occur every 1-15 minutes (enter 0 to disable):

```
config system global
   set sys-perf-log-interval <number from 0-15>
end
```

Add a field for the central NAT id to traffic log messages (257800)

Field name is '*centralnatid*'.

Add http.referrer url to web filter logs (260538)

Field name is '*referralurl*'.

Improve log viewer filters and bottom pane (258873)

The performance status message now shows useful information (254613)

Sample information looks like this, showing percentages and information:

'*Performance statistics: average CPU: 0, memory: 10, concurrent sessions: 8, setup-rate: 0*'

New log message whenever a NAT VDOM is restarted using execute router restart (267562)

Message is '*Router is manually restarted*'.

New GTP logs category (292096)

GTP logs are now handled separately from default Event logs, because of the possible volume of GTP logging.

Maximum values changes

This chapter describes new maximum values changes in FortiOS 5.4.

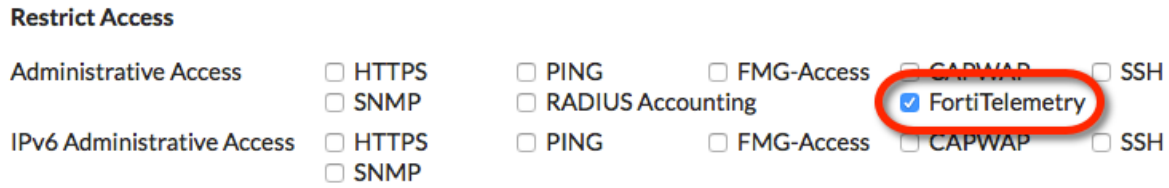
- Increase firewall.policy to 200,000 for 3000 series and above (367574)
- switch-controller.vlan removed from tablesize (370187)
- Changes to VM models max values (307672)
- IPv6 firewall virtual IP-related values changed to match IPv4 firewall virtual IP values. (263999)
- FortiOS Carrier GTP IMSI/APN maximum values increased 50,000 per VDOM. (252723)
- Maximum number of VLANs per interface for the FortiGate/FortiWiFi-30 models increased to 20 VLANs per physical interface. (300032)

Networking

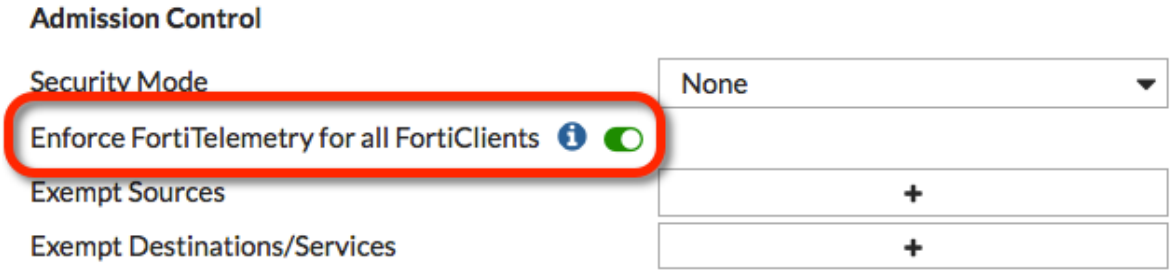
This chapter describes new network features added to FortiOS 5.4.

FortiTelemetry replaces FortiClient Access and other FortiClient interface settings (372945 299371)

To configure an interface to listen for connections from devices with FortiClient installed, enable **FortiTelemetryAdministrative Access**. FortiTelemetry was called FCT-Access or FortiClient Access in FortiOS 5.2.



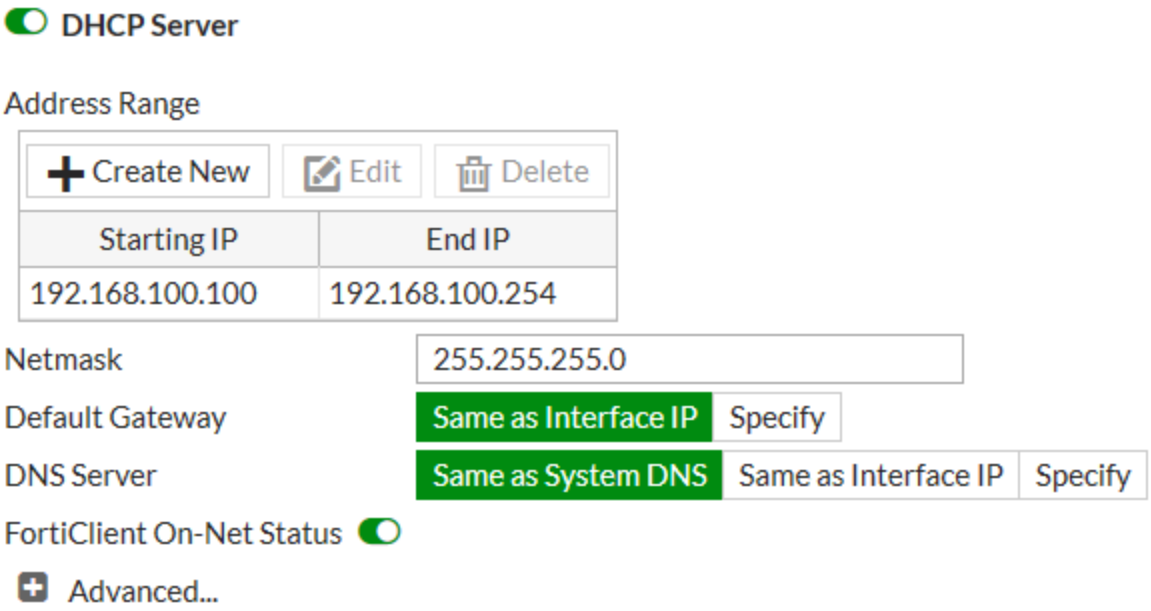
After enabling FortiTelemetry, under **Admission Control** you can select **Enforce FortiTelemetry for all FortiClients** to require clients to have FortiClient installed to be able to get access through the FortiGate. If you enable this feature you should also go to **Security Profiles > FortiClient Profiles** and configure FortiClient Profiles. Then you should add the configured FortiClient Profiles to firewall policies with device detection.



Use the following CLI command to enable FortiHeartBeat on an interface and enable enforcing FortiHeartBeat for all FortiClients:

```
config system interface
   edit port1
      set listen-forticlient-connection enable
      set endpoint-compliance enable
   end
```

After enabling FortiTelemetry, you can also enable **DHCP server** and turn on **FortiClient On-Net Status** to display the on-net status of FortiClient devices on the FortiClient Monitor (go to **Monitor > FortiClient Monitor**).



Use the following CLI command to enable FortiClient on-net status for a DHCP server added to the port1 interface:

```
config system dhcp server
   edit 1
      set interface port1
      set forticlient-on-net-status enable
   end
```

There was a name change involved with this feature. For 5.4.0, it was refered to as FortiHeartBeat, but this only appears in the 5.4.0 GA version of the FortiOS firmware.

TLS support for Dynamic DNS Services (DDNS) (300231)

This feature is available on the FortiGate 140-POE

When clear-text is disable, the FortiGate will use ssl connection to send and receive updates to Dynamic DNS services.

To disable clear-text:

```
config system ddns
   set clear-text disable
   end
```

The ssl-certificate name can also be set in the same location using the command:

```
   set ssl-certificate <cert_name>
```

Defaults:

- clear-text =`enable`
- ssl-certificate = `Fortinet_Factory`

DDNS update override for DHCP (306525 290048)

This feature is available on the FortiGate 140-POE

DHCP server now has an override command option, which allows DHCP server communications to go through DDNS to do updates for the DHCP client.

- This will force a DDNS update of the AA field every time even if the DHCP client does not request it.
- This will allow the support of the allow/ignore/deny client-updates options.

Syntax:

```
config system dhcp server
   edit 0
      set ddns-update_override [enable | disable]
      end
```

disable	Disable DDNS update override for DHCP
enable	Enable DDNS update override for DHCP

Enable or disable individual static and policy routes (174956)

CLI support has been added to [enable | disable] Static and Policy routes.

Syntax for static route in IPv4:

```
config route static
   edit 0
      set status [enable|disable]
      end
```

Syntax for static route in IPv6:

```
config route static6
   edit 0
      set status [enable|disable]
      end
```

Syntax for policy route in IPv4:

```
config router policy
   edit 0
      set status [enable|disable]
      end
```

Syntax for policy route in IPv6:

```
config router policy6
   edit 0
      set status [enable|disable]
      end
```

New option to allow copying of DSCP value in GRE tunnels (306331)

DSCP stands for the Differentiated services code point found in IPv4 and IPv6 headers, used for classifying and managing network traffic such as it relates to Quality of Service. This feature enables the keeping of the DSCP marking in the packets after encapsulation for going through GRE tunnels.

New DHCPv6 Prefix hint feature (302304)

This feature is used to "hint" to upstream DCHPv6 servers a desired prefix length for their subnet to be assigned in response to its request.

There is a possibility of duplicate prefixes being sent by ISP when using a /64 bit subnet because the first 64 bits of the address are derived from the mac address of the interface. This could cause an issue if the system administrator wishes to divide the host networks into 2 /64 bit subnets.

By receiving a /60 bit (for example) network address, the administrator can then divide the internal host works without the danger of creating duplicate subnets.

Also included in the new feature are preferred times for the life and valid life of the DHCP lease.

DHCPv6 hint for the prefix length

`set dhcp6-prefix-hint` <DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server>

DHCPv6 hint for the preferred life time.

`set dhcp6-prefix-hint-plt` <integer> 1 ~ 4294967295 seconds or "0" for unlimited lease time

DHCPv6 hint for the valid life time.

`set dhcp6-prefix-hint-vlt` <integer> 1 ~ 4294967295 seconds or "0" for unlimited lease tim

The FortiOS DHCP server now has an increased number of DHCP option fields (307342)

In place of specific fields the DHCP server now maintains a table for the potential options. The FortiOS DHCP server supports upto a maximum of 30 custom options.These optional fields are set in the CLI.

To get to the DHCP server:

```
config system dhcp server
   edit <integer - ID of the specific DHCP server>
```

To configure the options:

```
config options
```

Once in the options context, a few new configuration commands are available. First create an ID for the table entry:

```
edit <integer>
   set code <integer between 0 - 4294967295 to determine the DHCP option>
   set type [ hex | string | ip ]
   set value <option content for DHCP option types hex and string>
   set ip <option content for DHCP option type ip>
end
```

New option to dedicate a FortiGate interface to connect to a managed FortiSwitch (294607)

When setting up an interface, an additional option has been added to the potential addressing modes that dedicates the interface to being the connection to a FortiSwitch.This is covered in more detail in the FortiSwitch section.

New CLI option to change the maximum number of IP route cache entries (363410)

The maximum number of route cache entries is configurable.

Syntax:

```
config system global
   set max-route-cache-size <integer between 0 - 2147483647>
   end
```

Unsetting the field will cause the value to be set to the kernel calculated default.

```
config system global
   unset max-route-cache-size
   end
```

Support for 802.1x fallback and 802.1x dynamic VLANs (308012)

There are 4 modes when enabling 802.1x on a virtual switch interface:

Default	In this mode, it works as it did previously.
Fallback	In fallback mode, the virtual switch will be treated as a master. Only one slave can refer to a fallback master. Those ports in the master virtual switch are always authorized. After passing 802.1x authentication, the ports will be stay authorized and moved to its slave virtual switch.
Dynamic-vlan	In dynamic-vlan mode, the virtual switch will also be treated as a master. However, many slaves can refer to a dynamic-vlan master. Those ports in the master virtual switch are always un-authorized. After passing 802.1x/MAB authentication, the ports will be set to authorized and moved to one of its slave virtual switches.
Slave	In slave mode, a master must be set through security-8021x-master attribute. A slave virtual switch will use its master virtual switch's security-groups settings for authentication.

CLI example for fallback mode

```
config system virtual-switch
   edit "fallsw"
      set physical-switch "sw0"
      config port
   end
   edit "trust"
      set physical-switch "sw0"
   end
config system interface
   edit "fallsw"
      set vdom "root"
      set ip 192.168.20.1 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm auto-ipsec radius-acct probe-
          response capwap
      set type hard-switch
      set security-mode 802.1X
      set security-8021x-mode fallback(fallback mode master switch)
```

```
      set security-groups "rds-grp"(the usergroup for 802.1x)
      set snmp-index 10
      next
   edit "trust"
      set vdom "root"
      set ip 192.168.22.1 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm auto-ipsec radius-acct probe-
          response
      set type hard-switch
      set security-mode 802.1X
      set security-8021x-mode slave(slave mode switch)
      set security-8021x-master "fallsw" (its master switch)
      set snmp-index 6
      next
   end
```

CLI example for dynamic-vlan mode

```
config system virtual-switch
   edit "internal"
      set physical-switch "sw0"
   edit "lan-trust"
      set physical-switch "sw0"
      next
   edit "lan-vlan1000"
      set physical-switch "sw0"
      next
   edit "lan-vlan2000"
      set physical-switch "sw0"
      config port
      edit "internal1" (normally we should not add port in slave switch. This is used if
          user wants to manually add one port in slave)
      end
   end
config system interface
   edit "internal"
      set vdom "root"
      set ip 192.168.11.99 255.255.255.0
      set allowaccess ping https ssh http fgfm capwap
      set type hard-switch
      set security-mode 802.1X
      set security-8021x-mode dynamic-vlan<------dynamic-vlan mode master switch
      set security-groups "rds-grp"<------the usergroup for 802.1x
      set snmp-index 15
      next
   edit "lan-trust"
      set vdom "root"
      set ip 192.168.111.99 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm auto-ipsec radius-acct probe-
          response capwap
      set type hard-switch
      set security-mode 802.1X
      set security-8021x-mode slave<-----slave mode switch
      set security-8021x-master "internal"<-----its master switch
      set snmp-index 7
      next
   edit "lan-vlan1000"
      set vdom "root"
```

```
        set ip 192.168.110.1 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm auto-ipsec radius-acct probe-
            response capwap
        set type hard-switch
        set security-mode 802.1X
        set security-8021x-mode slave<-----slave mode switch
        set security-8021x-master "internal"<-----its master switch
        set security-8021x-dynamic-vlan-id 1000 <-----the matching vlan id for this virtual
            switch
        set snmp-index 16
        next
    edit "lan-vlan2000"
        set vdom "root"
        set ip 192.168.220.1 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm auto-ipsec radius-acct probe-
            response capwap
        set type hard-switch
        set security-mode 802.1X
        set security-8021x-mode slave
        set security-8021x-master "internal"
        set security-8021x-dynamic-vlan-id 2000
        set snmp-index 17
        end
    config user group
        edit "rds-grp"
            set dynamic-vlan-id 4000(default vlan id if there is no vlan attribute return
                from server)
            set member "190"
        end
```

Internet-Service database (288672 281333 291858)

Go to ***Policy & Objects > Internet Service Database*** to view the Internet Service Database. The database contains detailed information about services available on the Internet such as DNS servers provided by Adobe, Google, Fortinet, Apple and so on and a wide range of other services. For each service the database includes the IP addresses of the servers that host the service as well as the port and protocol number used by each IP address.

Interfaces assigned to Virtual Wired Pairs don't have "roles" (296519)

Assigning an interface to be part of a virtual wire pairing will remove the "role" value from the interface.

STP (Spanning Tree Protocol) support for models with hardware switches (214901 291953)

STP used to be only available on the old style switch mode for the internal ports. It is now possible to activate STP on the hardware switches found in the newer models. These models use a virtual switch to simulate the old Switch Mode for the Internal ports.

The syntax for enabling STP is as follows:

```
config system interface
    edit lan
    set stp [enable | disable]
```

```
end
```

Command to determine interface transceiver optical signal strength (205138 282307)

The new `get system interface transceiver` command can be used to determine optical signal strength when using SFP/SFP+ modules. The command can be used for trouble shooting fiber optic connections to service providers. This command is hardware dependent and currently supported by FortiGate models that include various SFP/SFP+ interfaces including the FortiGate-100D/200D-POE/400D/500D/900D/1000D/1200D/1500D/3700D/3700DX) models.

New command to get IPv6 multicast router information (267650)

The following command displays IPv6 multicast router information just like the IPv4 version of the command.

```
get router info6 multicast.
```

FortiGate DHCP works with DDNS to allow FQDN connectivity to leased IPs (267043)

As clients are assigned IP addresses, they send back information that would be found in an A record to the FortiGate's DHCP server, which can take this information and passes it back to a corporate DNS server so that even devices using leased IP address can be reached using FQDNs. The settings for this feature are configured through the CLI using the ddns-update command and some other ddns related options.

Fortinet's Dynamic DNS services (FortiDDNS) can be registered to a public IP address (251748)

Fortinet's Dynamic DNS services (FortiDDNS) can be registered to a public IP address even if the FortiGate itself does not have any physical interfaces on the Internet. This is applicable when the FortiGate is behind other networking devices that are employing NAT. This can be configured in the GUI as well as CLI.

Can use firewall addresses for static route destinations (273672)

To help prevent false positive when scanning for duplicate static routes, the dst_addr field is also checked.

Can use firewall addresses for policy route destinations (244101)

When configuring a policy route, firewall addresses and address groups can be used. The only exception for address types that can be used is the URL type of address object.

Enhance TWAMP Light functionality with server/controller functionality (249255)

TWAMP(Two-Way Active Measurement Protocol) Light is a simplified architecture within the TWAMP standard. Its purpose is to measure the round trip IP performance between any two devices within a network that supports the protocol. Now FortiOS operates in more than just the role of responder/reflector.The server/controller functionality has been added.

More information about interface status available from GUI (240285)

The following information is added to the 'hover' details for each port on the GUI FortiGate faceplate:

- MAC address
- Tx/Rx bytes
- Tx/Rx packets
- Tx/Rx errors

In addition, optional columns are added to the interface list to allow users to see all of the above information.

Virtual WAN link fixes (255122)

The firmware now has the following fixes or improvements to Virtual WAN links (VWL):

- Better support for dynamic interfaces (PPPoE and DHCP).
  - It can remove dynamically added routes, and restore these routes once the interfaces are not members.
  - It can count pppoe interface sessions.
  - It can generate a proute for a PPPoE interface. In this proute, the gateway is specified, while the outgoing (PPPoE)interface will not set.
- Adjust the route policy for a manual mode VWL service
- Support HTTP monitor by version 1.1, which obsoletes version 1.0's behavior.
- Apply multiple dst and src new feature for one policy to VWL.
- Improvements to CLI usability:
  - It hides interfaces that are being used in a policy or a zone
  - There is a check when adding an interface to a static route. This check will raise an error if the interface is a member of a VWL.
  - Updates a proute, if based on config change, if the associated link-monitor dies.
  - Fix some inappropriate messages.
  - Revised the minimum value of interval for a link-monitor object. The new value is 1, so it can be compatible with V5.0. When the timeout is 1, and interval is 1.

Router > Static > Settings GUI options available from the CLI only

As part of the new WAN Load Balancing feature, the FortiOS 5.2 **Router > Static > Settings** GUI page has been removed. WAN Load Balancing should be used instead of the 5.2 **ECMP Load Balancing Method** settings. The 5.2 **Link Health Monitor** definitions are now only available from the CLI.

Ports preassigned as sniffer ports by default (261921)

Some models of FortiGate, by default have ports preconfigured as sniffer ports.

The models and ports preconfigered in sniffer mode are as follows:

- FortiGate 300D
  - Port4
  - Port8
- FortiGate 500D
  - Port5
  - Port6
  - Port13
  - Port14

Enable or disable inspecting IPv4 and IPv6 ICMP traffic (258734)

In order for the inspection of assymetric ICMP traffic to not affect TCP and UDP traffic, a pair of settings have been added that can enable/disable the inspection of ICMP traffic being routed assymetricly for both IPv4 and IPv6.

The syntax in the CLI for configuring the setting is:

- IPv4

```
config system settings
   set asymroute-icmp
   end
```

- IPv6

```
config system settings
   set asymroute6-icmp
   end
```

Send GARP on aggregate MAC change (273363)

FortiGates will send out GARP (Gratuitous Address Resolution Protocol) announcements if the MAC address of a link aggregated interface has changed to a new IP pool address due to a link failure or change in ports. This is needed when using networking devices, such as some switches, that don't perform this function when they receive LACP (Link Aggregation Control Protocol) information about changes in the MAC information.

Support split ports (252444)

The 5001D 40 GB can be split into 4 10 GB ports.This is done through a combination of hardware and software configuration. A specific 40 GB connector is used to connect to the 40 GB port and normally, the other end of the fibre optic cable would connect to another 40 GB port but a special cable can be used that is a single 40 GB connector at one end and 4 10 GB connections at the other. To use this set up the port also has to be configured to be a split port.

The configuration option can be found in the CLI:

```
config system global
   set port-split port1 port2
   end
```

The ports will be checked to make sure that they are not in use or referenced by other policy configurations. If in use the command will be aborted. Changing the port to be a split port will require a system reboot.

Add FortiClient enforcement to interfaces (253933)

The use of FortiClient can be enforced on individual interfaces. Go to **Network > Interfaces** and pick the interface of your choice. Under the heading **Admission Control**, you can enable the setting **Allow FortiClient Connections**.Once this setting is enabled, two more options become visible, **Discover Clients (Broadcast)** and **FortiClient Enforcement**. By enabling FortiClient Enforcement you enforce that in order for incoming traffic to pass through that interface it must be initiated by a device running FortiClient.

Once the use of FortiClient is enforced on the interface, FortiClient profiles should also be configured for the incoming connections. You can also set up any exemptions that are needed. Just below the **FortiClient**

Enforcement option are fields for **Exempt Sources** and **Exempt Destinations/Services**. These can be selected from address or services object already configured on the FortiGate.

In the CLI the enforcement can be set up as follows:

```
config system interface
   edit port1
      set listen-forticlient-connection [enable|disable]
      set endpoint-compliance [enable|disable]
      end
```

Botnet C&C protection added to interfaces (254959)

The function of Botnet and Command & Control traffic protection is not new but how it can be configured has changed. It is no longer part of the AntiVirus Security profile.

The option to **ScanOutgoing Connections to Botnet Sites** has been added to the Interface page in the GUI.

The options are **Disable**, **Block** and **Monitor.**

In the CLI, the botnet scan can be configured on the interface by entering the following commands:

```
config system interface
   edit <interface>
      set scan-botnet-connections [disable | block | monitor]
      end
```

It is also possible to enable the scanning of botnet and C&C traffic in

- Firewall policies

```
config firewall policy
   edit <policyid>
      set scan-botnet-connections [disable | block | monitor]
      end
```

- Firewall explicit proxy policies

```
config firewall explicit-proxy-policy
   edit <policyid>
      set scan-botnet-connections [disable | block | monitor]
      end
```

- Firewall interface policy

```
config firewall interface-policy
   edit <policyid>
      set scan-botnet-connections [disable | block | monitor]
      end
```

- Firewall sniffer

```
config firewall sniffer
   edit <policyid>
      set scan-botnet-connections [disable | block | monitor]
      end
```

Netflow 9.0 support (167405)

Netflow is a networking feature introduced by Cisco to collect and export information about traffic flow through routers. IPFIX (Internet Protocol Flow Information Export) is the standardized Internet Protocol based on NetFlow

version 9. The standards requirements for IPFIX are outlined in RFC 3197 and its basic specifications and other information are documented in RFC 5103, RFC 6759 and RFC 7011 through RFC 7015.

The CLI changes that enable and configure "NetFlow" traffic are:

```
config system netflow
   set collector-ip <collector IP>
   set collector-port <NetFlow collector port>
   set csource-ip <Source IP for NetFlow agent>
   set cactive-flow-timeout <time in minutes of timeout to report active flows>
   set cinactive-flow-timeout <time in seconds of timeout for periodic report of finished
       flows>
   end
```

These setting can also be configured per VDOM by going to:

```
config system vdom-netflow
```

A Netflow sampler will also have to be enabled on specific interfaces.

IPv6 blackhole static routing (220101)

System administrators use black hole routing to divert undesirable traffic, such as packets from a Denial of Service (DoS) attack or communications from an illegal source. The traffic is routed to a dead interface, or a host designed to collect information for investigation. This mitigates the impact of the attack on the network.

The use of blackhole routing is enabled in the CLI as follows:

```
config router static6
   edit <ID #>
      set blackhole enable
   end
```

A collection of Routing changes (261043)

A few new settings have been added to the CLI to assist in the supporting of the IPsec Auto Discovery feature. They are designed for:

- The support of the RIPng (RIP next generation) network command
- Limiting the maximum metric allowed to output for RIPng
- Fix NSM missing kernel address update info

The actual new settings are:

```
config router rip
   set max-out-metric <integer value 1 - 15>
   end


config router ripng
   set max-out-metric <integer value 1 - 15>
   end


config router ripng
   config network
      edit <ID # of network>
         set prefix <IPv6 prefix>
         end
      end
```

DHCPv6 prefix delegation (266061)

Prefix delegation is now support for DHCP for IPv6 addressing. It is not practical to manually provision networks on a large scale in IPv6 networking. The DHCPv6 prefix delegation feature is used to assign a network address prefix, and automate the configuration and provisioning of the public routable addresses for the network.

Enabling the prefix delegation is done only in the CLI as in the following example:

```
config system interface
   edit "wan1"
      config ipv6
         set ip6-mode dhcp
         set ip6-allowaccess ping
         set dhcp6-prefix-delegation enable
         end
      end
```

Proxy-arp extensions (250651)

The proxy-arp configuration can be extendend to an IP address range rather than a single IP address. A new setting has been added to the CLI. When configuring the proxy-arp, in addtion to setting the IP address, an end-ip address can also be set. If it is not set, the proxy-arp will be a single address as before. An example configuration using the new setting would be a follows:

```
config system proxy-arp
   edit 1
      set interface "internal"
      set ip 192.168.1.100
      set end-ip 192.168.1.102
      end
```

Routing

Add asymmetric route for icmp/icmp6:

Adding asymmetric route for icmp/icmp6 without effecting tcp/udp.

Enhance TWAMP Light functionality with server/controller functionality

Add support for twamp lite mode for both controller and responder site.

CLI changes:

Add twamp protocol as a probe protocol in the link-monitor CLI.

```
config vdom
   edit root
      config system link-monitor
         edit lnkmt1
            set protocol twamp //TWAMP link monitor.
         end
```

```
end
```

Route Lookup

Route Lookup is under **Router > Monitor > Routing Monitor**, the input criteria are **Destination IP address/FQDN**, and an enable check box for **IPv6**.

After clicking on **Search** button, the trace result will be selected on routing monitor page with highlight.

RFCs supported by FortiOS 5.4

The following RFCs are now supported by FortiOS 5.4:

RFC 2231 MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations (280039)

RFC 7507 TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks (308040)

Improve support for RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE) (213945)

RFC 4106 The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)

RFC 4303 IP Encapsulating Security Payload (ESP) (255144)

RFC 4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)

RFC 4478 Repeated Authentication in Internet Key Exchange (IKEv2) Protocol (282025)

RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA) (0206110)

RFC 5176 Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) (239028)

RFC 5177 Network Mobility (NEMO) Extensions for Mobile IPv4 (249570)

RFC 5723 Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption (289914)

RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2) (255144)

RFC 6106 IPv6 Router Advertisement Options for DNS Configuration (266061)

RFC 6290 A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE) (298970)

RFC 6888 Common Requirements for Carrier-Grade NATs (CGNs)

RFC 7539 ChaCha20 and Poly1305 for IETF Protocols (264785)

RFC 4787 Network Address Translation (NAT) Behavioral Requirements for Unicast UDP (229074)

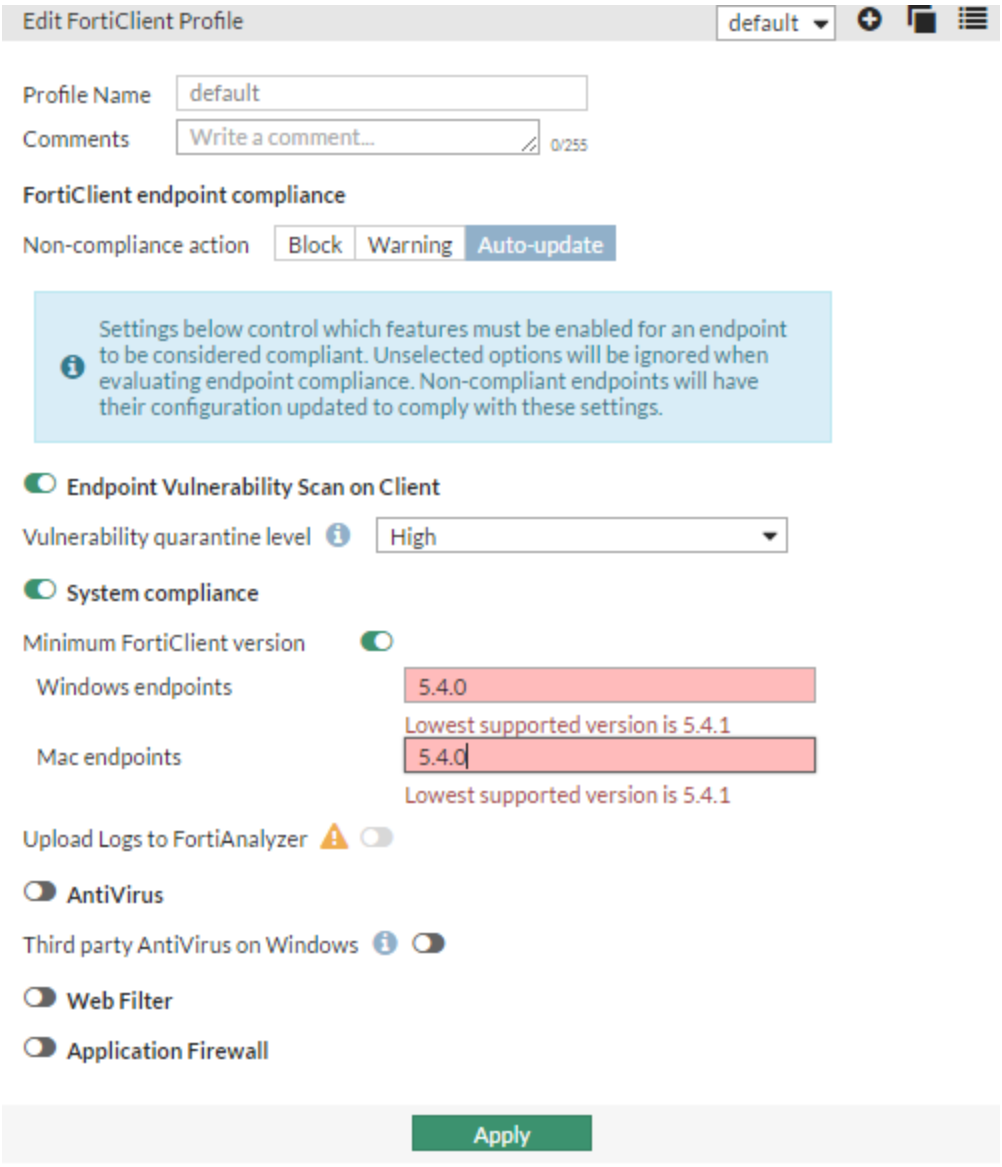
Security Profiles

This chapter describes new security profile features added to FortiOS 5.4.

FortiClient Profile changes (356205)

Features involving general settings have been removed from the FortiClient profile GUI in 5.4.1. Features emphasizing compliance of the endpoint devices have been added. These enhancements facilitate integration with the Cooperative Security Fabric.

When FortiClient endpoint compliance is enabled and FortiClient endpoints are registered to FortiGate, you must upgrade registered FortiClient endpoints. Be sure to upgrade registered endpoints to FortiClient 5.4.1 before upgrading your FortiGate to FortiOS 5.4.1.



FortiClient endpoint compliance enforcement has three actions. When the action is set to **Block** or **Warning**, it is up to you to provision endpoints either via the Enterprise Management Server (EMS) or manually. When the action is set to **Auto-update**, the FortiGate will provision the endpoint.

Action	Meaning
Block	If the endpoint does not match compliance rules in the FortiClient Security Profile, then it will be blocked.
Warning	If the endpoint does not match compliance rules in the FortiClient Security Profile, then it will show on the Monitor > FortiClient Monitor as not-compliant. Traffic will not be blocked.
Auto-update	If the endpoint is not-compliant, the FortiGate will push a limited profile to the endpoint and attempt to get it to be compliant.

CLI syntax

A third value called **compliant** and new attributes have been added to existing CLI.

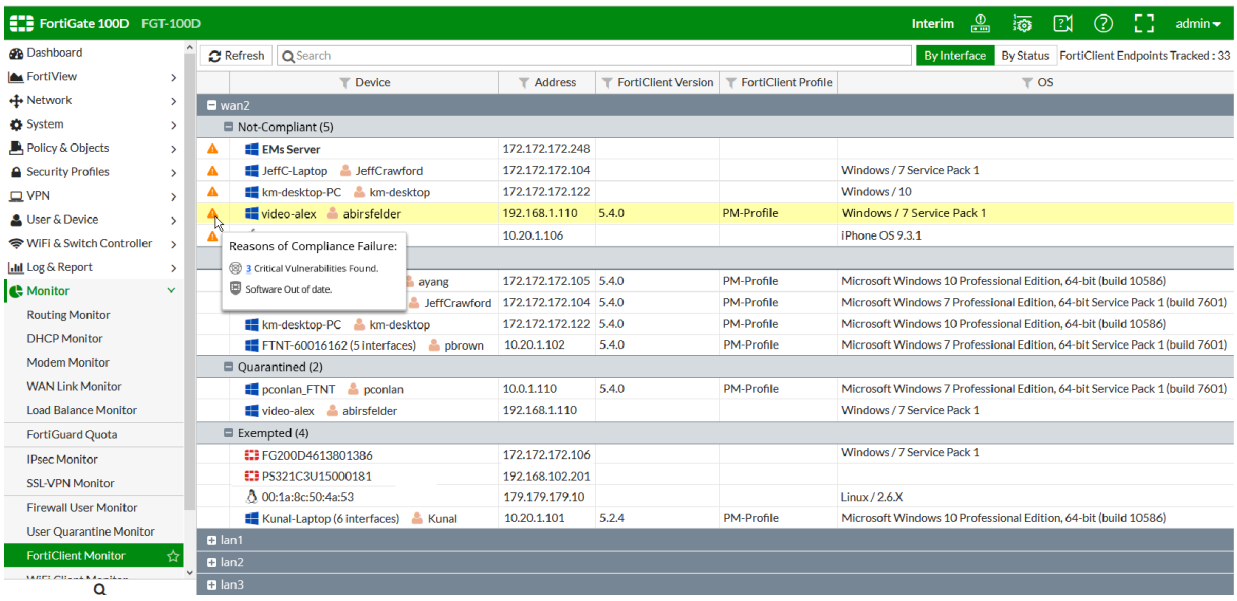
```
config endpoint-control profile
   edit <profile name>
      config forticlient-winmac-settings
         set compliance-action {block | warning | auto-update}
         set os-av-software-installed {enable | disable}
         set forticlient-log-upload-level {traffic | vulnerability | event}
         set forticlient-system-compliance {enable | disable}
         set forticlient-minimum-software-version {enable | disable}
         set forticlient-vuln-scan-enforce {enable | disable}
         set forticlient-vuln-scan-enforce-grace {0 - 30 days, default = 1}
         set sandbox-analysis {enable | disable}
      end
   end
```

FortiClient Monitor page updates (304254)

Updates to the **Monitor** page allow the user to view FortiClient endpoint devices grouped by interface and then sub-grouped by compliance status. Compliance status can be compliant, non-compliant, exempt, or quarantined.

	FortiClient Enforcement	
Status	**Enabled**	**Disabled**
Compliant	List only active FortiClientEndpoints.	No devices listed
Not-compliant	List devices not-compliant with FortiClient profile, so long as they are not exempt.	No devices listed
Exempt	List FortiClient endpoints exempt from FortiClient compliance.	List of all user devices except those quarantined by the administrator.
Quarantined	List devices quarantined by the administrator.	List devices quarantined by the administrator.

You can see the reasons for non-compliance by right-clicking on an endpoint in the list.



FortiClient Endpoint Control Profile Attributes (306833)

Certain attributes have been removed from, added to, or changed in the FortiClient endpoint control profile configuration.

Attributes Removed

You can no longer configure these attributes in the FortiClient endpoint control profile:

```
view-profile-details
scan-download-file
wait-sandbox-result
use-sandbox-signature
block-malicious-website
block-attack-channel
av-scheduled-scan
av-scan-type
av-scan-schedule
av-scan-time
av-scan-exclusions
monitor-unknown-application
install-ca-certificate
disable-wf-when-protected
forticlient-vuln-scan-schedule
forticlient-vuln-scan-on-registration
forticlient-vpn-provisioning
forticlient-advanced-vpn
forticlient-advanced-vpn-buffer
disable-unregister-option
forticlient-log-ssl-upload
forticlient-log-upload-schedule
forticlient-update-from-fmg
forticlient-update-server
forticlient-update-failover-to-fdn
forticlient-settings-lock
forticlient-settings-lock-passwd
```

```
   auto-vpn-when-off-net
   auto-vpn-name
   client-log-when-on-net
   forticlient-ad
   fsso-ma
   fsso-ma-server
   fsso-ma-psk
   allow-personal-vpn
   disable-user-disconnect
   vpn-before-logon
   vpn-captive-portal
   forticlient-ui-options
   forticlient-advanced-cfg
   forticlient-advanced-cfg-buffer
```

Attributes Added

The following attributes have been added to the FortiClient endpoint control profile configuration.

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set sandbox-analysis {enable | disable}
      set compliance-action {block | warning | auto-update}
      set os-av-software-installed {enable | disable}
      set forticlient-minimum-software-version {enable | disable}
      set forticlient av {enable | disable}
      set forticlient-system-compliance {enable | disable}
      set forticlient-log-upload
      set forticlient-log-upload-level {traffic |vulnerability | event}
      set forticlient-vuln-scan-enforce {enable | disable}
      set forticlient-vuln-scan-enforce-grace {number}
   end
end
```

Attributes Changed

There is a change to the CLI commands to enable or disable the sending of files to FortiSandbox for analysis.

The CLI command:

```
config endpoint-control profile
   edit <name_str>
   config forticlient-winmac-settings
      edit <name_str>
         set sandbox-scan {enable | disable}
      end
   end
```

has been replaced by:

```
config endpoint-control profile
   edit <name_str>
   config forticlient-winmac-settings
      edit <name_str>
         set sandbox-analysis {enable | disable}
```

```
    end
end
```

Optionally include FortiGuard spam responses in email log messages (284055)

The field **FortiGuard Spam Response** has been added as an option to the anti-spam log to aid in identifying misclassified email.

Virus scanning of MS Outlook email (308797)

FortiOS 5.4.1 allows users to enable or disable inspection of MAPI-over-HTTP (MAPI/HTTP) protocol. This protocol was first delivered with Outlook 2013 SP1 and Exchange 2013 SP1. Enabling inspection ensures that the FortiGate can scan Outlook email for viruses.

CLI commands

```
config firewall ssl-ssh-profile
   edit deep-inspection
   set mapi-over-https {enable|disable}
```

Improved Visibility of Botnet and Command & Control (C&C) protection (308104)

Mobile & Botnet C&C license information is now displayed in the License Information widget in the Dashboard. Additionally, you can view the list of Botnet C&C packages in the IP Reputation Database (IRDB) and the Botnet Domain Database (BDDB) from the License Information widget.

A button has been added to the GUI on the DNS filter page allowing you to block DNS requests known to FortiGuard. When you enable this feature, you can open a definitions window by clicking on "botnet package."

Access to the IRDB is available to users through FortiCare support contracts purchased or renewed before October 1, 2016. After that date, users will have to subscribe to the IRDB either through the FortiGuard Mobility Security Service (FMSS) or the FortiGuard Enterprise Bundle.

DLP changes (297960)

Some DLP features removed. DLP fingerprinting removed from the GUI.

FortiClient Endpoint Profile improvements and new features (285443 275781 287137)

- **275781:** New options available in **FortiClient Profiles**.
- **285446:** VPN can be configured on the GUI either on **IPsec VPN** or **SSL-VPN** and changes can be preserved.
- **287137:** In the **Mobile** tab, .mobileconfig files can be configured and **Client VPN Provisioning** can be enabled.

Features involving general settings have been removed from the FortiClient profile GUI in 5.4.1. Features emphasizing compliance of the endpoint devices have been added. Read FortiClient Profile changes for more information.

FortiClient Enforcement added to Interfaces (253933)

FortiClient enforcement has been moved from the Policy page to **Network > Interfaces** to enforce FortiClient registration on a desired LAN interface rather than a policy.

To enforce FortiClient endpoint registration - GUI:

1. Go to **System > Feature Select** and enable **Endpoint Control**.
2. Go to **Network > Interfaces** and select the internal interface.
3. Under **Restrict Access**, enable **FortiTelemetry**.
4. Under **Admission Control**, enable **Enforce FortiTelemetry for all FortiClients**.

FortiClient exempt list improvements (268357 293191)

- **268357:** Before you could only configure captive portal policy addresses in the CLI, but it can now be performed in the GUI.
- **293191: Exempt List** has been replaced with **Exempt Sources**, and **Exempt Destinations/Services** has been added (once an interface has been set to captive portal). Before it was only possible to configure the FortiGate interface port to captive portal through the CLI, but it can now also be performed in the GUI.

FortiClient endpoint profile page updates (283968)

The **Security Profiles > FortiClient Profiles** page has been redesigned to better present the information available, and so the user can easily locate particular settings of interest.

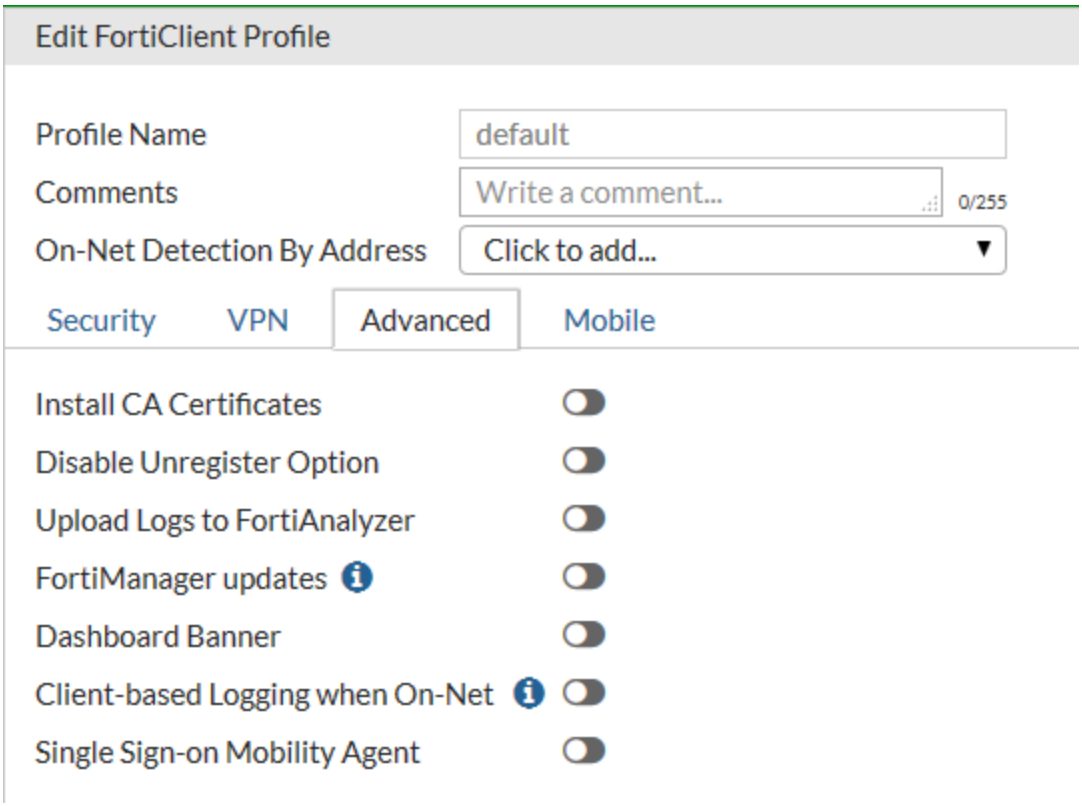
Pre-existing GUI options under **User & Device > FortiClient Profiles** have been moved to the **Security Profiles** menu, and have been reorganized into separate tabs: **Security**, **VPN**, **Advanced**, and **Mobile**. Profiles can be created and options can be enabled within these tabs.

The **VPN**, **Advanced**, and **Mobile** tabs do not appear in the GUI in FortiOS5.4.1. See FortiClient Profile changes (356205).

Note that **Client-based Logging when On-Net** has been renamed to **Allow Access to Logs from FortiClient Console**.

In addition, the following features were added:

- Support for FortiSandbox integration
- Option for C&C destination scanning and blocking
- Certificate deployment as part of endpoint profile
- FortiClientRTP Option updates
- Option to monitor all unknown applications



Configure the ability to store FortiClient configuration files (171380)

1. Enable the advanced FortiClient configuration option in the endpoint profile:

```
config endpoint-control profile
   edit "default"
      set forticlient-config-deployment enable
      set fct-advanced-cfg enable
      set fct-advanced-cfg-buffer "hello"
      set forticlient-license-timeout 1
      set netscan-discover-hosts enable
   next
end
```

2. Export the configuration from FortiClient (xml format).
3. Copy the contents of the configuration file and try to paste in the advanced FortiClient configuration box.

If the configuration file is greater than 32k, you need to use the following CLI:

```
config endpoint-control profile
   edit <profile>
      config forticlient-winmac-settings
         config extra-buffer-entries
            edit <entry_id>
               set buffer xxxxxx
            next
         end
      end
   end
```

FortiOS 5.4 no longer supports FortiClient 5.0 or earlier (289455)

FortiOS 5.2 would support FortiClient 5.0 (only if the FortiGate upgraded to FortiOS 5.2), however FortiOS 5.4 will no longer support FortiClient 5.0. Customers need to purchase a FortiClient 5.4 subscription-based FortiClient license.

Session timers for IPS sessions (174696 163930)

The standard FortiOS session time-to-live (session TTL) timer for IPS sessions has been introduced to reduce synchronization problems between the FortiOS Kernel and IPS. This has been added so that FortiGate hard-coded timeout values can be customized, and IPS was using too much overall memory.

Botnet protection with DNS Filter (293259)

The new botnet list from FortiGuard can be used to block DNS requests to known botnet C&C IP addresses within a new DNS filter profile.

You can view the botnet list by going to **System > FortiGuard > Botnet Definitions**.

Secure white list database (288365)

Secure white list exemption for SSL deep inspection. To enable, go to **Security Profiles > SSL/SSH Inspection** and enable **Exempt from SSL Inspection** and enable **Reputable Websites**.

Mobile Malware protection update (288022)

Mobile Malware protection requires a separate license and can be downloaded as a separate object. The mobile malware signatures are no longer part of the AntiVirus Database but these signatures can be enabled by going to **Security Profiles > AntiVirus** and enabling **Include Mobile Malware Protection**.

Options not supported by the new quick mode flow-based virus scanning (288317)

Files cannot be sent to FortiSandbox for inspection while in quick mode flow-based virus scanning, and so the GUI option for it has been removed. No option to switch between quick mode and full mode, as choice between **Proxy** and **Flow** based inspection has been removed.

Add mobile malware to FortiGuard licenses page and include more version information (290049)

An entry and version information for **Mobile Malware Definitions** has been added in the **License Information** table under **System > FortiGuard**. Also, main items have been bolded and sub-items have been indented for clarification.

Secure white-list DB for flow based UTM features (287343)

A new feature that gathers a list of reputable domain names that can be excluded from SSL deep inspection. This list is periodically updated and downloaded to FortiGate units through FortiGuard.

Syntax:

```
config firewall ssl-ssh-profile
   edit deep-inspection
      set whitelist enable
end
```

New customizable replacement message that appears when an IPS sensor blocks traffic (240081)

A new replacement message will appear specifically for IPS sensor blocked Internet access, to differentiate between IPS sensor blocking and application control blocking.

Low-end models don't support flow AV quick mode and don't support the IPS block-malicious-url option (288318)

AV quick mode and the IPS block-malicious-url option have been disabled on low-end FortiGate models, however these features can be enabled if the FortiGate unit has a hard disk. Low-end models will only support**Full**scan mode (the option is left in the GUI to show which mode is active for the user).

New quick mode flow-based virus scanning (281291)

When configuring flow-based virus scanning you can now choose between quick and full mode. Full mode is the same as flow-based scanning in FortiOS 5.2. Quick mode uses a compact antivirus database and advanced techniques to improve performance. Use the following command to enable quick mode in an antivirus profile:

```
config antivirus profile
   edit <profile-name>
      set scan-mode {quick | full}
   end
```

CVE-IDs now appear in the FortiOS IPS signature list (272251)

The signature list can be found at **Security Profiles > Intrusion Protection > View IPS Signatures**.

Botnet protection added (254959)

The latest Botnet database is available from FortiGuard. You can see the version of the database and display its contents from the **System > FortiGuard** GUI page. You can also block, monitor or allow outgoing connections to Botnet sites for each FortiGate interface.

FortiSandbox URL database added

You can see the version of the database and display its contents from the **System > FortiSandbox** GUI page.

New Web Filter profile whitelist setting and changes to blacklist setting (283855, 285216)

Domain reputation can now be determined by "common sense", for sites such as Google, Apple, and even sites that may contain sensitive material that would otherwise be trusted (i.e. there is no risk of receiving botnets or

malicious attacks). You can tag URL groups with flags that exempt them from further sandboxing or AV analyzing.

You can identify reputable sites and enable certain bypasses under **Security Profiles > Web Filter**.

Similarly, you can exempt the identified reputable sites from SSL inspection.

CLI Syntax

```
config firewall ssl-ssh-profile
   edit <profile-name>
      set whitelist [enable | disable]
end

config webfilter profile
   edit <profile-name>
      config web
      set whitelist exempt-av exempt-webcontent exempt-activex-java-cookie exempt-dlp
          exempt-rangeblock extended-log-others
      end
end
```

Support security profile scanning of RPC over HTTP traffic (287508)

This protocol is used by Microsoft Exchange Server so this feature supports security profile features such as virus scanning of Microsoft Exchange Server email that uses RPC over HTTP.

Users now allowed to override blocked categories using simple, wildcard, and regex expressions to identify the URLs that are blocked (270165)

This feature is also called per-user BWL. To be able to configure this feature from the GUI enter the following command:

```
config system global
   set per-user-bwl enable
end
```

Then go to **Security Profiles > Web Filtering**, edit a web filtering profile and select **Allow users to override blocked categories**.

Use the following command to configure this feature from the CLI:

```
config webfilter profile
   edit <profile-name>
      set options per-user-bwl
   end
```

Set flow or proxy mode for your FortiGate (or per VDOM) (266028)

You can configure your FortiGate or a VDOM to apply security profile features in proxy or flow mode. Change between modes from the System Information dashboard widget. Proxy mode offers the most accurate results and the greatest depth of functionality. Flow mode provides enhanced performance. IPS and application control always operates in flow mode and so is not affected by changing this mode.

Security Profiles > Web Application Firewall

Signatures can now be filtered based on risk level.

The options to reset action and apply traffic shaping is now only available in the CLI.

The *All Other Known Applications* option has been removed, while the option for *All Other Unknown Applications* has been renamed *Unknown Applications*.

Block all Windows executable files (.exe) in email attachments (269781)

A new option has been added to AntiVirus profiles to block all Windows executable files (.exe) in email attachments.

CLI Syntax

```
config antivirus profile
   edit "default"
      config imap
         set executables {default | virus}
      end
      config pop3
         set executables {default | virus}
      end
      config smtp
         set executables {default | virus}
      end
      config mapi
         set executables {default | virus}
      end
   end
```

Cookies can now be used to authenticate users when a web filter override is used (275273)

Cookies can be used to authenticate users when a web filter override is used. This feature is available in CLI only.

CLI Syntax

```
config webfilter cookie-ovrd
   set redir-host <name or IP>
   set redir-port <port>
end

config webfilter profile
   edit <name>
      config override
         set ovrd-cookie {allow | deny}
         set ovrd-scope {user | user-group | ip | ask}
         set profile-type {list | radius}
         set ovrd-dur-mode {constant | ask}
         set ovrd-dur <duration>
         set ovrd-user-group <name>
         set profile <name>
```

```
      end
   end
```

Blocking malicious URLs (277363)

A local malicious URL database dowloaded from FortiGuard has been added to assist IPS detection for live exploits, such as drive-by attacks. You enable blocking malicious URLs in an IPS profile from the CLI using the following command:

CLI Syntax

```
config ips sensor
   edit default
      set block-malicious-url {enable | disable}
   next
end
```

The FortiGuard IPS/AV update schedule can be set by time intervals (278772)

This feature allows updates to occur more frequently (syntax below shown for updates randomly every 2-3 hours).

CLI Syntax

```
config system autoupdate schedule
   set frequency every
   set time 02:60
end
```

Application Control signatures belonging to industrial category/group are excluded by default (277668)

Use the following command to be able to add industrial signatures to an application control sensor:

```
config ips global
   set exclude-signatures {none | industrial}
end
```

The Industrial category now appears on the Application Control sensor GUI.

An SSL server table can now be used for SSL offloading (275273)

CLI Syntax

```
config firewall ssl-ssh-profile
   edit <name>
      set use-ssl-server {enable | disable}
   next
end
```

MAPI RPC over HTTP/HTTPS traffic is now supported for security scanning (278012)

CLI Syntax

```
config firewall profile-protocol-options
   edit "default"
      set comment "All default services."
         config http
            set ports 80 3128
            set options rpc-over-http
         end
      end
```

New Dynamic DNS FortiGuard web filtering sub-category (276495)

A new FortiGuard web filtering sub-category, Dynamic DNS, has been added and can be found in the Security Risk Category. Also, the sub-category *Shopping and Auction* has been separated into two sub-categories: *Auction* and *Shopping.*

New Filter Overrides in the Application Sensor GUI (260901)

The overrides allow you to select groups of applications and override the application signature settings for them.

FortiGate CA certificates installed on managed FortiClients (260902)

This feature allows you to enable or disable CA certificate installation on managed FortiClients in a FortiClient Profile.

Syntax

```
config endpoint-control profile
   edit <profile>
      config forticlient-winmac-settings
         set install-ca-certificate [enable | disable]
      end
   next
end
```

More exemptions to SSL deep inspection (267241)

Some common sense exemptions have been added to the default SSL deep inspection profile, such as Fortinet, Android, Apple, Skype, and many more.

Exempting URLs for flow-based web filtering (252010)

You can once again exempt URLs for flow-based web filtering.

Filter overrides in Application Sensors (246546)

In the Application Sensor page, a new section named **Filter Overrides** has been introduced. From this section, clicking **Add Filter/Edit Filter** will launch a dialog to pick/edit the advanced filter and save it back to the list.

New keyword byte_extract for custom IPS and Application Control signatures (179116)

The new `byte_extract` custom IPS signature key has been added that supports snort-like byte extraction actions. It is used for writing rules against length-encoded protocols. The keyword reads some of the bytes from the packet payload and saves it to a variable. You can use the `-quiet` option to suppress the reporting of signatures.

IPS logging changes (254954)

IPS operations severely affected by disk logging are moved out of the quick scanning path, including logging, SNMP trap generation, quarantine, etc.

Scanning processes are dedicated to nothing but scanning, which results in more evenly distributed CPU usage. Slow (IPS) operations are taken care of in a dedicated process, which usually stays idle.

New FortiGuard web filtering category: Dynamic DNS (265680)

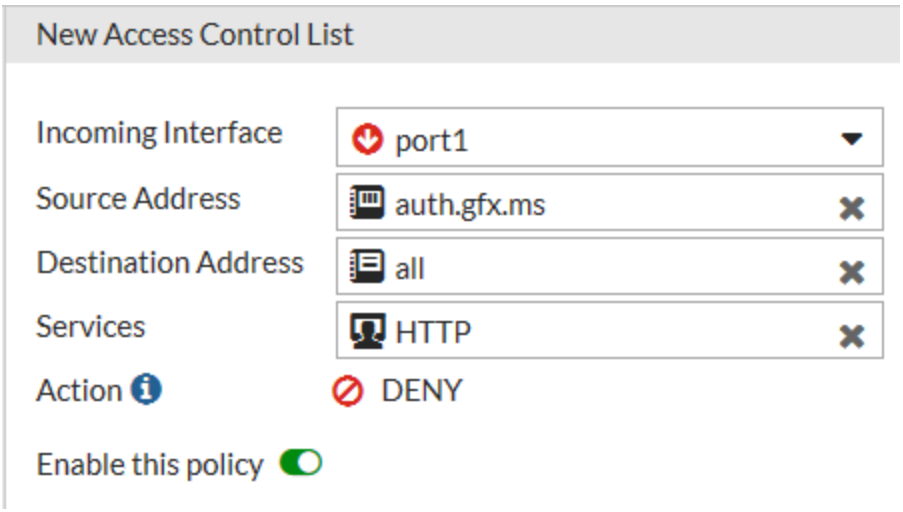
A new FortiGuard web filtering category has been added for **Dynamic DNS** under the **Security Risk** heading, to account for nearly half a million URLs of "Information Technology" rated by BlueCoat as "Dynamic DNS Host".

Syntax

```
config webfilter profile
   edit <profile>
      config ftgd-wf
         config filters
            edit <id>
               set category 88<--- New category, Dynamic DNS; number 88
         end
   end
end
```

Access Control Lists in DoS Policies (293399)

You can go to **Policy & Objects > IPv4 Access Control List** or **Policy & Objects > IPv6 Access Control List** and select an incoming interface and add a list of Firewall source and destination addresses and services and drop traffic that matches.



You can use the following CLI command to add an ACL:

```
config firewall acl
   edit 1
      set interface "port1"
      set srcaddr "google-drive"
      set dstaddr "all"
      set service "ALL"
   next
end
```

Websense web filtering through WISP (287757)

WISP is a Websense protocol that is similar in functionality to ICAP, it allows for URLs to be extracted by a firewall and submitted to Websense systems for rating and approval checking.

This feature provides a solution for customers who have large, existing, deployed implementations of Websense security products to replace their legacy firewalls with a Fortigate family, such that they are not forced to make a change to their web filtering infrastructure at the same time.

In order to use Websense's web filtering service, a WISP server per VDOM needs to be defined and enabled first. A Web filtering profile is then defined that enables WISP, which in turn is applied to a firewall policy.

When WISP is enabled, the FortiGate will maintain a pool of TCP connections to the WISP server. The TCP connections will be used to forward HTTP request information and log information to the WISP server and receive policy decisions.

Syntax

```
config web-proxy wisp
   set status enable
   set server-ip 72.214.27.138
   set max-connection 128
end

config webfilter profile
   edit "wisp_only"
      set wisp enable
   next
```

```
end
```

Other new Security Profiles features:

- CPU allocation & tuning commands now remain after a system reboot (276190)
- The GUI notifies an administrator when the FortiGate is in conserve mode (266937)
- A new custom IPS signature option, "--ip_dscp" has been added to be compatible with engine 1.x. (269063)
- The RTP/RTSP decoder can now detect slave sessions (273910)
- ISNIFF can now dump all HTML files if the dump-all-html CLI command is used (277793)
- Sender and recipient fields have been added to flow-based SMTP spam logs (269063)
- Browser Signature Detection added to Application Control profiles (279934)

Session-aware Load Balancing (SLBC)

GUI support for SSL VPN and WiFi controller in SLBC mode (246481)

SSL VPN and WiFi controller GUI pages now appear on the worker GUI when operating in SLBC mode.

Add an option to force IPsec to use NAT Traversal (275010)

Add a new option for NAT. If NAT is set to forced, then the worker will use a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC.

SSL VPN

This chapter describes new SSL VPN features added to FortiOS 5.4.

Control the cipher suites that can be used by an SSL VPN (304741)

Administrators can now ban the use of specific cipher suites in the CLI for SSL VPN, so PCI-DSS (Payment Card Industry Data Security Standard) certification can be met.

CLI syntax

```
config vpn ssl settings
   set banned-cipher [RSA | DH | DHE | ECDH | ECDHE | DSS | ECDSA | AES | AESGCM |
       CAMELLIA | 3DES | SHA1 | SHA256 | SHA384]
```

SSL VPN monitor enhancements (258700)

SSL VPN monitor GUI page is updated, with additional usability improvements.

Change to SSL VPN authentication (306982)

SSL VPN authentication has been refined to fix an issue regarding authentication policies being ignored.

Local and remote users with multiple groups and policies will authenticate with the first matched policy (user in policy has higher priority), and traffic will go through all matched policies.

Significant SSL VPN web portal improvements (287328, 292726, 299319)

Significant updates and improvements have been made to the SSL VPN web portal in preparation for future browser updates, and in order to support all browsers:

- SSL VPN web portal redesigned.
- SSL VPN tunnel mode widget no longer works in the web portal. The tunnel mode widget used a deprecated NPAPI plugin mechanism to send the tunnel client to the browser for local system execution—this is a popular exploitation vector. FortiClient is now required for tunnel mode SSL VPN.
- SSL VPN Web mode RDP Native java applet removed.
- Removed unnecessary options from RDP bookmark and changed to HTML5 RDP.
- Cache cleaning function has been removed.
- If updating to 5.4.1, see above (258700).

Implement post-authentication CSRF protection in SSL VPN web mode (287180)

This attribute can enable/disable verification of a referrer in the HTTP request header in order to prevent a Cross-Site Request Forgery attack.

Syntax:

```
config vpn ssl settings
```

```
   set check-referer [enable|disable]
end
```

Group-based SSL VPN bookmarks (292125)

This CLI-only feature allows administrators to add bookmarks for groups of users. SSL VPN will only output the matched group-name entry to the client.

Syntax:

```
config vpn ssl web portal
   edit "portal-name"
      set user-group-bookmark enable*/disable
   next
end
config vpn ssl web user-group-bookmark
   edit "group-name"
      config bookmark
         edit "bookmark1"
         ....
         next
      end
   next
end
```

DTLS support (227138)

The Datagram Transport Layer Security (DTLS) protocol is supported for SSL VPN connections. DTLS support can be enabled in the CLI as described below.

Syntax

```
config vpn ssl settings
   set dtls-tunnel [enable | disable] (default: enabled)
end
```

Added options to allow firewall addresses to be used in routing table for SSL VPN (265430)

If destination **Named Address** is set in **Network > Static Routes** and **Address Range** is set to **Automatically assign addresses** in **VPN > SSL-VPN Settings**, SSL VPN should refresh the routing table automatically.

HTTP to HTTPS redirect support (278728)

The admin HTTP port can now be redirected to the admin HTTPS port. This is enabled in **VPN > SSL-VPN Settings** using the option **Redirect port 80 to this login port**.

There are two likely scenarios for this:

- SSL VPN is not in use, in which case the admin GUI runs on port 443 or 10443, and port 80 is redirected.
- SSL VPN runs on port 443, in which case port 80 is redirected to 443 and the admin port runs on 10443.

If the administrator chooses to run SSL VPN on port 80, the redirect option is invalid.

This can also be configured in the CLI as described below.

Syntax:

```
config vpn ssl settings
   set https-redirect [enable | disable] (default: disabled)
end
```

Removed guest group and SSO group (303041)

Guest group and SSO group have been removed from `config user group` and `config vpn ssl web user-group-bookmark`.

CLI changes (299319)

Removed the following obsolete/unnecessary portal options from the CLI:

```
config vpn ssl web portal
   edit <name>
      set auto-prompt-mobile-user-download   REMOVED
      set display-forticlient-download   REMOVED
      set display-history-limit   REMOVED
      set page-layout   REMOVED
      set cache-cleaner   REMOVED
   end
```

Removed the following unnecessary RDP bookmark options from the CLI in preparation for HTML5 RDP:

```
config vpn ssl web <user-bookmark|user-group-bookmark>
   edit <group/user name>
      config bookmarks
         edit <bookmark>
            set full-screen-mode   REMOVED
            set screen-height   REMOVED
            set screen-width   REMOVED
            set keyboard-layout   REMOVED
         end
      end
```

System

This chapter describes new system administration features added to FortiOS 5.4.

Incorrect access group for backup and restore config (389328)

FortiOS no longer allows lower level administrator profiles to backup and restore the FortiOS configuration (because this would allow them to acquire hashes for administrator passwords, including super-admin).

Enhancements to IPS Signatures page (285543)

The IPS signatures list page now shows which IPS package is currently deployed. Users can also change their IPS package by linking directly to the FortiGate's **System > FortiGuard** page from the IPS Signatures list page.

Combine multiple commands into a CLI alias (308921)

Multiple commands can be supported under a single command alias defined in the CLI by users.

Configure alias command

```
config system alias
   edit "alias-name" -- Alias command name
      set command "get system status" -- Command list to execute
   next
end
```

Basic config examples (simple command substitution)

```
config sys alias
   edit 1
      set alias "sh ver"
      set cmd "get system status"
   next
   edit 2
      set alias "sh ip route"
      set cmd "get router info routing-table all"
   next
   edit 3
      set alias "sh bgp sum"
      set cmd "get router info bgp summary"
   next
   edit 11
      set alias "debug1"
      set cmd "diag debug enable;diag debug flow show console enable"
   next
   edit 12
      set alias "debug2"
      set cmd "diag debug flow filter saddr"
      set noenter enable
   next
   edit 13
      set alias "debug3"
```

```
      set cmd "diag debug flow trace start"
      set noenter enable
   next
   edit 14
      set "alias debugstop"
      set "cmd diag debug flow trace stop"
   next
end
```

Advanced config examples (parameter substitution)

```
config sys alias
   edit 4
      set alias "sniff (\d+\.\d+\.\d+\.\d+)"
      set cmd "diag sniffer packet any 'host $1' 4"
   next
   edit 5
      set alias "sniff6 (\d+\.\d+\.\d+\.\d+)"
      set cmd "diag sniffer packet any 'host $1' 6"
   next
   edit 6
      set alias "sniff (\S+) (.*)"
      set cmd "diag sniffer packet $1 '$2' 4"
   next
   edit 7
      set alias "trace (\d+\.\d+\.\d+\.\d+) (\d+)"
      set cmd "diag debug enable;diag debug flow show console enable;diag debug flow
          filter saddr $1;diag debug flow trace start $2"
   next
end
```

The `noenter` setting specifies whether the alias substitution should contain a new line or not.

These examples are placed in numerical order.

.

New SNMP trap for bypass events (307329)

When bypass mode is enabled or disabled on FortiGate units that are equipped with bypass interfaces and support AMC modules, a new SNMP trap is generated and logs bypass events.

Maintainer password recovery enhancements (356944)

For information about recovering a lost password and enhancements to the process, see: Resetting a lost Admin password on the Fortinet Cookbook site.

SSH support updated to 7.1p1 (290889)

The OpenSSH daemon has been upgraded from version 3.7.1p2 to version 7.1p1 to support new security algorithms.

The central management FortiGuard server list can include FQDNs (354449)

This new feature implements support of FQDN, to make it an option for central-management server-list. This feature can be set through the GUI and the CLI.

GUI Changes

On **System > FortiGuard > Override FortiGuard Servers > Create New / Edit**, a new option, **FQDN** is added for **Address Type**.

CLI Changes

```
config server-list
   edit 1
      set server-type {update|rating}
      set addr-type {ipv4|ipv6|fqdn} <== added fqdn
      set server-address ipv4
      set server-address6 ipv6
      set fqdn FQDN <== added
   end
```

Features removed from the FortiGate 80C (356154)

Features have been changed on the FortiGate / FortiWifi 80C so as to increase available memory and decrease the image size on flash.

Changes made include:

- removal of web application firewall (WAF)
- removal of WAN optimization
- removal of network vulnerability scan (netscan)
- compression of the Intrusion Prevention System and AntiVirus library files and storing them in a gzip file
- compression of certain WiFi data files
- addition of virtual switch function for 80c (applicable to 5.4 only)

New role property on interfaces (294385)

Interfaces now have a property called 'role' which affects visibility and suggests different default options depending on it's value.

- WAN - this interface is used to connect to the internet.
- LAN - this interface is used to connect to local network of endpoints.
- DMZ - this interface is used to connect to servers.
- Undefined - This interface has a custom role which isn't one of the above.

Interface roles affect visibility of properties and features (295736)

Depending on an interfaces role, some properties may set to a default value and the visibility of others may be set to show or hide in the GUI.

Toggle automatic authorization of extension devices (294966)

When an interface is configured to be dedicated to an extension device, a new option appears to auto-authorize extension devices.

Support for new modem added (293598)

Support for the Linktop LW273 modem has been added.

IPS packet capture files can be backed up (276489)

Use the command `execute backup disk ipsarchives` and the option of `tftp`, `ftp`, or `usb`.

Change between NAT and Transparent modes removed from the GUI (278289)

The feature in the GUI initiating the change between NAT and Transparent modes has been removed. It can still be done, but only through the CLI. The configuration setting that is used is:

```
config system settings
   set opmode [nat | transparent]
   end
```

Switch mode changes (286447)

Hub mode is no longer available. The old switch mode, usually called 'LAN' will no longer be available. The interface mode is still available and on all models, and instead of the old switch mode, most of the lower end units will come configured, by default, with a hardware switch called 'LAN', which has the function of the old switch mode but is more flexible. Most models with 40 ports or more will come by default in vlan switch mode.

New start attribute as been added to scheduled scripts (285206)

The start attribute has the options manual and auto. Manual means a schedule script needs to be manually started after a reboot. Auto automatically restarts the script after a reboot.

Use the following command to set a script to automatically run after the FortiGate starts up:

```
config system auto-script
   edit <script-name>
      set start auto
   end
```

Toggle displaying the hostname on the GUI login page (272572)

Use the following command:

```
config sys settings
```

```
    set gui-display-hostname {disable | enable}
end
```

PPTP and L2TP address pool ranges expanded (275709)

PPTP and L2TP address pool ranges are allowed to use a subnet mask of up to 255.255.0.0 (B-class), increasing the maximum range size from 254 to 65,534

Pop up notification of impending timeout of Administrator GUI sessions (266413)

A convenience feature to let administrators know that their session is about to expire. This is especially convenient for units that have a timeout setting of just a few minutes.

SNMP can generate traps based on detecting a device's online/offline status (273107)

This setting is related to the device detection feature. It allows SNMP traps to detect when a new device comes online. Within SNMP configurations there is a configurable timeout setting that periodically checks for the device. When a check determines that the device is present a trap is sent.

In the GUI, when configuring an SNMP object, one of the settings is a checkbox, under **SNMP Events** for **Device detected**.

To configure the SNMP object in the CLI use the following syntax:

```
config system snmp community
   edit <community ID number>
      set name <string>
      set events device-new
      end
```

In order to configure the idle timeout for the device, use the following syntax in the CLI:

```
config system global
   set device-idel-timeout <integer of time in seconds>
   end
```

The time value for the field can be set from 30 to 31536000.

SNMP improvements for dynamic routing (168927)

SNMP improvements for dynamic routing include support for RFC 4750 OSPF Version 2 Management Information Base and RFC 5643 Management Information Base for OSPFv3. These changes add the capability of logging dynamic routing activity. Examples include sending OSPF routing events or changes to a syslog server or FortiAnalyzer or changes in neighborhood status.

Network Mobility Extensions for Mobile IPv4 (NEMO)

This is an implementation of RFC 5177 that includes the following CLI command.

```
config system mobile-tunnel
   set status enable/disable //Enable/disable this mobile tunnel.
   set roaming-interface port1 //Roaming interface name.
   set home-agent xxx.xxx.xxx.xxx //IP address of the NEMO HA.
   set home-address xxx.xxx.xxx.xxx // Home IP address.
   set n-mhae-spi 256 //NEMO authentication spi.
```

```
    set n-mhae-key-type ascii/base64 //NEMO authentication key type.
    set n-mhae-key vWZZxx //NEMO authentication key.
    set hash-algorithm hmac-md5 //Hash Algorithm.
    set tunnel-mode gre //NEMO tunnnel mode.
    set renew-interval 60 //Time before lifetime expiraton to send NMMO HA re-registration.
    set lifetime 180 //NEMO HA registration request lifetime.
    set reg-interval 5 //NEMO HA registration interval.
    set reg-retry 3 //NEMO HA registration maximal retries.
end
```

Restoring configuration file without rebooting the FortiGate (237786)

A setting has been added in the CLI that when set to enable, will allow the FortiGate to start using the newly uploaded configuration file without going through a full reboot process.

The syntax for the setting is:

```
config system global
   set reboot-upon-config-restore {enable | disable}
end
```

Auto repeat of CLI commands(160023 259531)

Occasionally there is a need to repeatedly run a diagnose command over a long period of time (like checking CPU or memory usage, or checking proxy health), Previously, this could only be done with external console connections. Now this can be done in a script using the `interval` and `repeat` commands.

Scripts can be uploaded as a file from the CLI or GUI. To upload scripts from the GUI go to **System > Advanced > Configuration Scripts** and upload and run the script.

To configure the schedule and scripts, use the following syntax:

```
config system auto-script
   edit <ScriptName>
      set interval
      set repeat
      set script
   end
end
```

`interval` the interval time in seconds between instances of the script running.

`repeat` the number of times to repeat the running of the script. The value 0 is used to set an infinite number of repetitions.

`start` select `manual` to start the script manually or `auto` to start the script automatically

`script` the contents of the script.

This feature may not be available on all models as a hard drive is necessary to make use of it.

Proxy-arp function extension (250651)

A new attribute `end-ip` is added to proxy-arp. If `end-ip` is not set, then the ip has the same meaning as before. If `end-ip` is set, then the ip becomes the start-ip, and the `end-ip` should be larger than ip and the ip range should less than 256.

```
config system proxy-arp
   edit 1
      set interface internal
      set ip xxx.xxx.xxx.xxx
      set end-ip xxx.xxx.xxx.xxx
   next
end
```

Changes to the FortiGuard Distribution Network GUI page (219862)

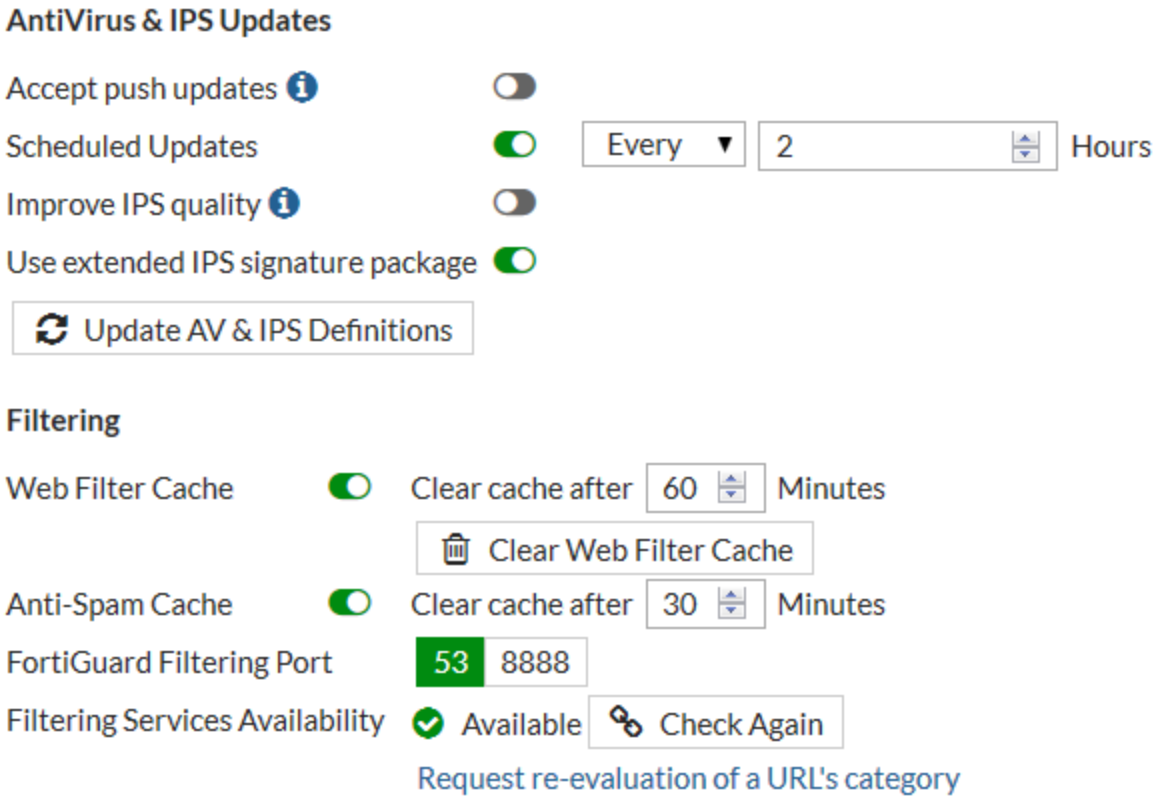
The **System > FortiGuard** page has been updated to include new FortiGuard features including Mobile Malware Definitions, Botnet Definitions and so on. From this page you can also upload packages, and view the list of Botnet Definitions.

FortiGuard Distribution Network

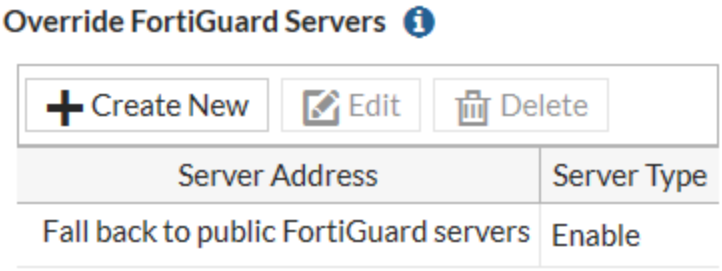
License Information

Contract	Status	
FortiCare Support	Registered (kleroux@fortinet.com)	Launch Portal
Hardware Version	8 x 5 support (Expires on 2016-09-29)	
Comprehensive Support	24 x 7 support (Expires on 2016-09-29)	
Firmware	8 x 5 support (Expires on 2016-09-29)	
Enhanced Support	24 x 7 support (Expires on 2016-09-29)	
IPS & Application Control	Licensed (Expires on 2016-09-29)	Upload Package
IPS Definitions	Version 6.00755	
IPS Engine	Version 3.00156	
AntiVirus	Licensed (Expires on 2016-09-29)	Upload Package
AV Definitions	Version 31.00354	
AV Engine	Version 5.00227	
Mobile Malware Definitions	Version 0.00000	
Botnet Definitions	Version 2.00684	View List
SSL-VPN Package	Unreachable	Upload Package
Web Filtering	Licensed (Expires on 2016-09-29)	
Anti-Spam Filtering	Licensed (Expires on 2016-09-29)	

From this page you can also access new functionality for AntiVirus and IPS updates and Web Filtering and Spam filtering.



You can also use this page to override FortiGuard servers.



Changes to firmware upgrade GUI page (248866)

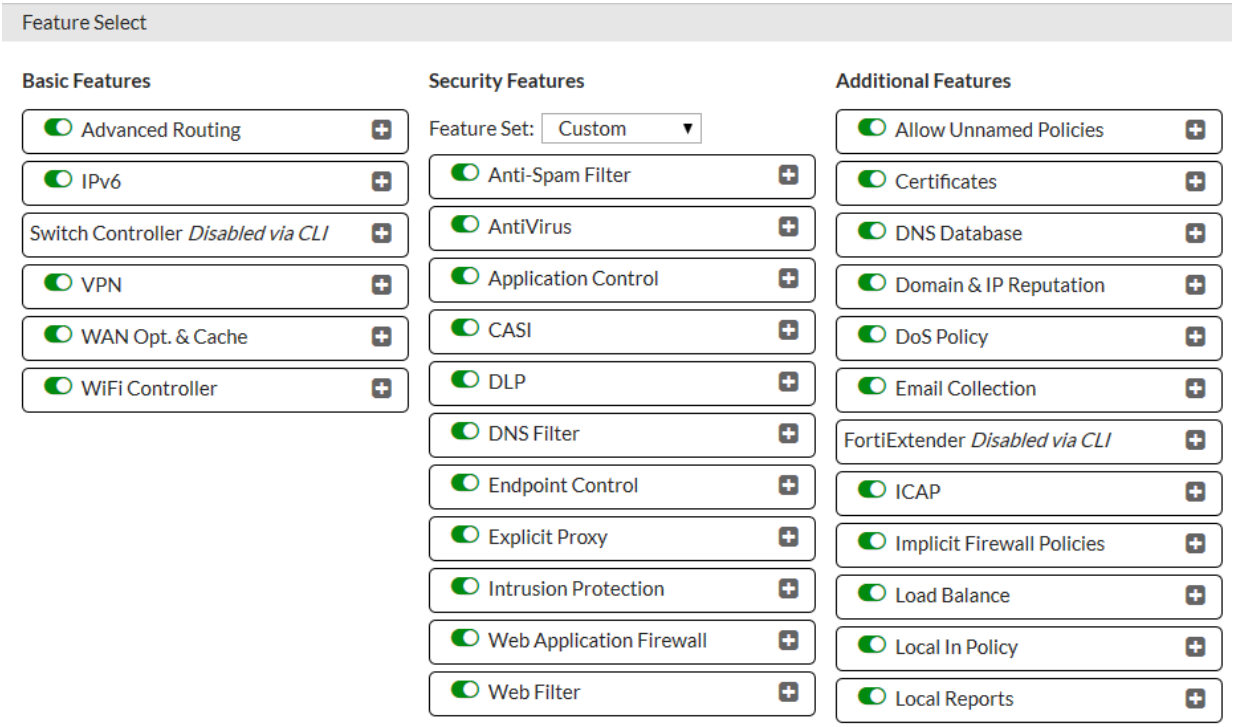
The following changes have been made to the GUI as it relates to the firmware upgrade process:

- The interface now provides an upgrade recommendations that is based on FortiGuard's list of supported upgrade paths
- Allows user to easily select and upgrade to one of the recommended versions
- There is a graphic representation of the progress of downloading the image and the upgrade process.

GUI features can now be enabled and disabled per VDOM (263708 273799)

When VDOMs are enabled, most of the items in the Features section of the menu are moved to a similar menu section within the VDOM menu and are now customizable on a per VDOM basis. Some items such as IPv6 and Certificates are still configured on a global basis.

From the GUI, you can enable or disable GUI features from **System > Feature Select**.

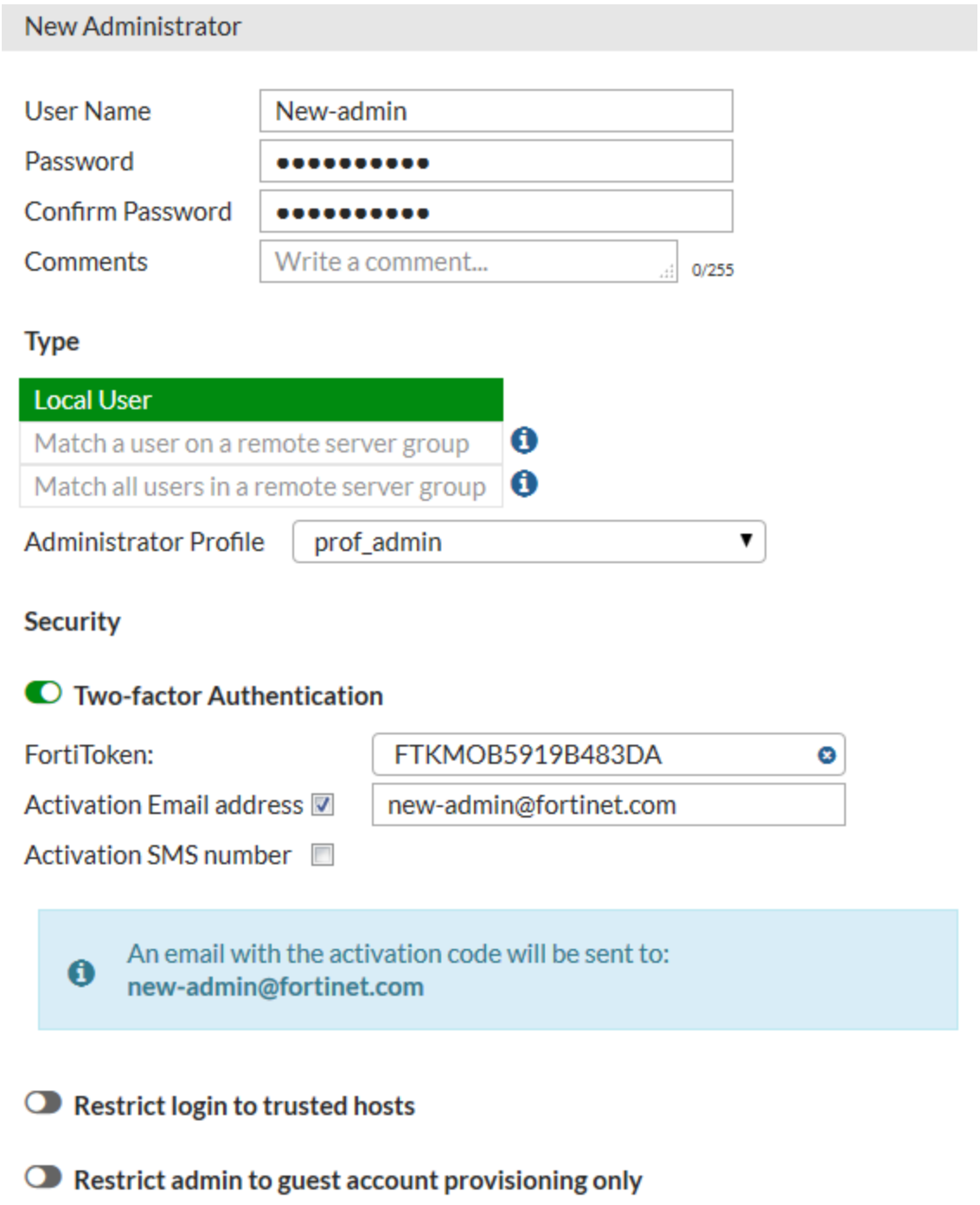


From the CLI, GUI items that are enabled or disabled per-VDOM are configured from the `config system settings` command. GUI items that are enabled globally are enabled or disabled from the `config system global` command.

Turning these features on or off does not enable or disable the feature but determines whether or not that option is displayed on the GUI.

Improvements to system admin GUI pages (205280)

Several items relating to system administration, and the configuration of the system administrator accounts and profiles in particular, have been updated so that the layout is clearer and more efficient. One of the things improve is that it is now easier to set up two factor authentication.



The TFTP session helper supports (263127)

The TFTP session helper supports TFTP for NAT66 and NAT46.

Support for IPv6 addressing when configuring central management (297144)

Previously, the configuration of an IP address for a server for ratings and updates, such as a FortiManager, could only use IPv4 addresses. Now, as shown below IPv6 addressing can be used as well.

```
config system central-management
   set type fortimanager
   set fmg "2000:172:16:200::207"
   set vdom "vdom1"
      config server-list
         edit 1
         set server-type rating update
         set addr-type ipv6
         set server-address6 2000:172:16:200::207
         next
      end
   end
```

New execute traceroute command options (272169)

Different query options can be configured for the `execute traceroute` command. These settings can also be saved using the `execute traceroute-options` command as follows:

```
execute traceroute-options device [Auto | <interface name>]
execute traceroute-options queries <integer>
execute traceroute-options source [Auto | <source interface IP address>]
```

The `queries` setting is to determine the number of queries per hop. Use execute traceroute-options to view the traceroute settings:

```
execute traceroute-options view-settings
Traceroute Options:
       Number of probes per hop: 3
       Source Address: auto
       Device: auto
```

Administrator password updates (292858)

To set a minimum level of security for the administrative accounts, minimum levels of complexity can be set on guest admin accounts.

```
config system password-policy-guest-admin
   set status [enable | disable]
   set min-lower-case-letter <integer>
   set min-upper-case-letter <integer>
   set min-non-alphanumeric <integer>
   set min-number <integer>
   end
```

If the required level of complexity is not met, an error message will appear explaining that the password must conform to the system password policy.

Certificate validation added to FortiGate email server configuration (299506)

When configuring the email server on a FortiGate to send out alert emails that use SMTPS, the FortiGate can validate the email chain, thus reducing the possibility of compromise.

In the CLI the configuration of the email is set up with the following syntax:

```
config system email-server
   set type custom
   set reply-to <email address>
   set server <SMTP server IP address or hostname>
   set port <integer for SMTP server port>
   set source-ip <SMTP server source address - IPv4 format>
   set source-ip6 <SMTP server source address - IPv6 format>
   set authenticate [enable| disable]
   set validate-server [enable| disable]
   security Connection security.
   set security [none | starttls |smtps|
   end
```

The `set validate-server` option is the new setting that enables the verification.

Changes to backing up and restoring configuration files (298176)

When you insert a USB drive into a FortiGate USB port options to save the configuration to USB and restore configuration from a USB appear on the configureation save and restore pages.

You can also use the command `execute backup usb` command to backup the configuration to the USB drive.

VDOMs

This chapter describes new VDOM features added to FortiOS 5.4.

Cooperative Security Fabric (CSF) firewalls do not support multiple VDOMs (365260)

This problem should be fixed in a future release.

VDOM name search added to GUI navigation (305221)

When selecting a VDOM you can search by name instead of manually searching through the entire list.

Stackable VDOM licenses (269153)

VDOM licenses are now stackable, allowing you to buy additional licenses and stack them on top existing licenses to increase the number of VDOMs you can have.

Support execution of global CLI commands from within VDOMs (262848)

A new CLI command, `sudo`, allows the running of global commands from within the vdom context of the CLI.This means that the user no longer has to:

1. exit from the VDOM
2. enter global
3. run the command
4. return to the previous VDOM

The syntax for the command is:

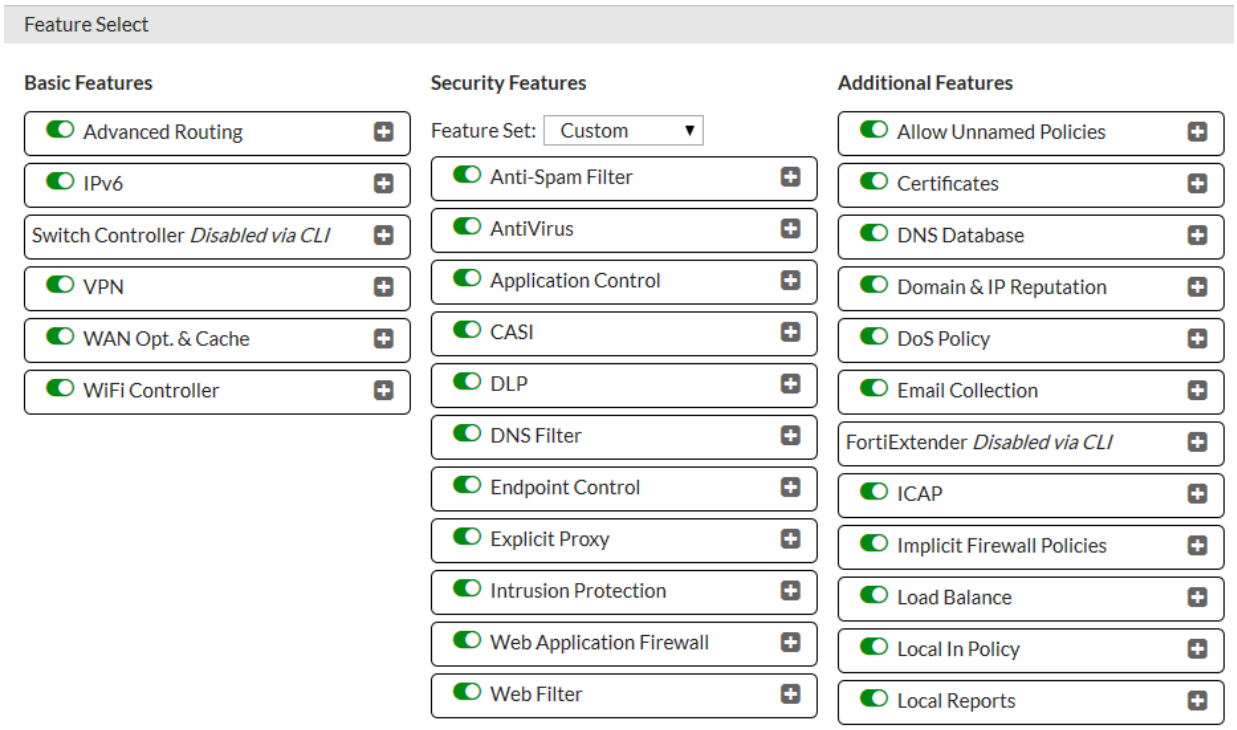
```
sudo {global | vdom-name} {diagnose | execute | show | get}
```

These commands will only work if the user already has permissions to run the command. Unlike the sudo command in some other operating systems like Linux, this command does not allow the user to run programs with the privileges of another user.

GUI features can now be enabled and disabled per VDOM (263708 273799 266028)

When VDOMs are enabled, most of the items in the Features section of the menu are moved to a similar menu section within the VDOM menu and are now customizable on a per VDOM basis. Some items such as IPv6 and Certificates are still configured on a global basis.

From the GUI, you can enable or disable GUI features from **System > Feature Select**.



From the CLI, GUI items that are enabled or disabled per-VDOM are configured from the `config system settings` command. GUI items that are enabled globally are enabled or disabled from the `config system global` command.

Turning these features on or off does not enable or disable the feature but determines whether or not that option is displayed on the GUI.

WAN Optimization

Toggle Disk Usage for logging or wan-opt (290892)

Both logging and WAN Optimization use hard disk space to save data. For FortiOS 5.4 you cannot use the same hard disk for WAN Optimization and logging.

- If the FortiGate has one hard disk, then it can be used for either disk logging or WAN optimization, but not both. By default, the hard disk is used for disk logging.
- If the FortiGate has two hard disks, then one disk is always used for disk logging and the other disk is always used for WAN optimization.

WAN Optimization is **not** supported while the FortiGate is in **Flow-based** inspection.

On the FortiGate, go to **System > Advanced > Disk Settings** to switch between **Local Log** and **WAN Optimization**.

You can also change disk usage from the CLI using the following command:

```
configure system global
   set disk-usage {log | wanopt}
end
```

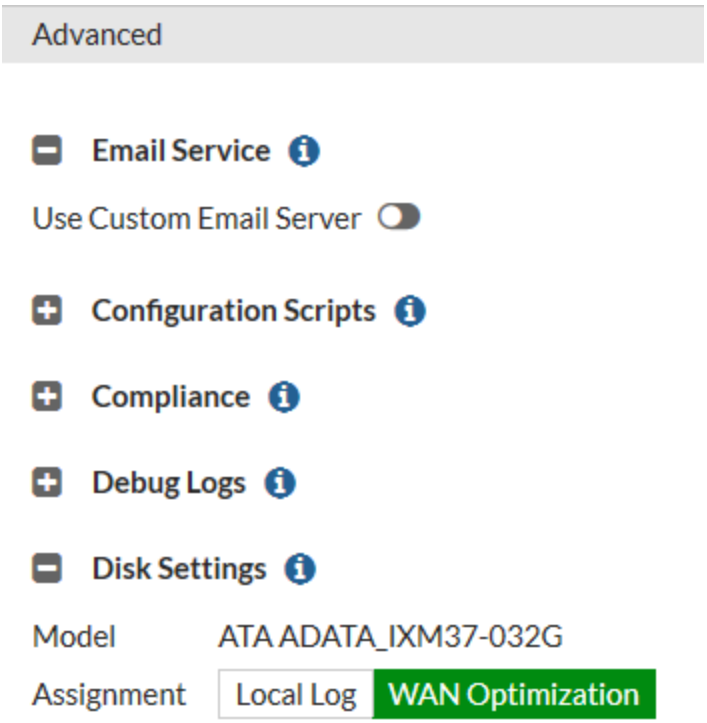
The Toggle Disk Usage feature is supported on all new "E" Series models, while support for "D" Series models may vary.

Please refer to the Feature Platform Matrix for more information.

Changing the disk setting formats the disk, erases current data stored on the disk and disables either disk logging or WAN Optimization.

You can configure WAN Optimization from the CLI or the GUI. To configure WAN Optimization from the GUI you must go to **System > Feature Select** and turn on WAN Optimization.

Remote logging (including logging to FortiAnalyzer and remote Syslog servers) is not affected by using the single local hard disk for WAN Optimization.



Enabling WAN Optimization affects more than just disk logging

In addition to affecting WAN Optimization, the following table shows other features affected by the FortiGate disk configuration.

Features affected by Disk Usage as per the number of internal hard disks on the FortiGate

Feature	Logging Only (1 hard disk)	WAN Opt. Only (1 hard disk)	Logging & WAN Opt. (2 hard disks)
Logging	Supported	Not supported	Supported
Report/Historical FortiView	Supported	Not supported	Supported
Firewall Packet Capture (Policy Capture and Interface Capture)	Supported	Not supported	Supported
AV Quarantine	Supported	Not supported	Supported
IPS Packet Capture	Supported.	Not supported	Supported
DLP Archive	Supported	Not supported	Supported

Feature	Logging Only (1 hard disk)	WAN Opt. Only (1 hard disk)	Logging & WAN Opt. (2 hard disks)
Sandbox DB & Results	FortiSandbox database and results are also stored on disk, but will not be affected by this feature.		

MAPI AV scanning is supported over WAN Optimization (267975)

AV works on MAPI when WAN Optimization is used.

WiFi

This chapter describes new WiFi features added to FortiOS 5.4.

Conflicting local-standalone and local-bridging VAP CLI resolved (256450)

- Disabling local-bridging now forcefully disables local-standalone. Also, disabling either local-bridging or local-standalone now forcefully disables intra-vap-privacy.
- Enabling intra-vap-privacy now forcefully disables local-standalone.
- Local-bridging will be forcefully enabled when local-standalone is also enabled.

Support fast-roaming for mesh backhaul link (274007 293321)

Added basic functionality required to make a leaf FortiAP able to roam fast enough from one root FortiAP to another when signal conditions change. The feature allows administrator to tune the fast roaming for most mobility scenarios. The leaf FAP is used as a wireless bridge passing traffic from the Ethernet port to the wireless mesh link.

- Includes background scan while the leaf AP is connected to the root AP (Mesh uplink established)
- Leaf AP will schedule a background scan using local interfaces (wbh0/1)
- Scan parameters are configured in the AP
- Every 10 minutes, WTP daemon reviews list of available root AP. If a better root AP is found, WTP daemon triggers a mesh roaming.

For full leaf AP scan mesh CLI variables, see Mesh variables on page 1.

Captive portal authentication to support roaming (284202 306681)

Client devices will maintain captive portal authentication as they roam across different APs. By maintaining a consistent authentication, a client can ensure uninterrupted access to latency sensitive applications such as VoIP.

Cloud will push a random per-APNetwork encrypt key to AP. The encrypt key is 32 bytes length, and will be used in captive portal fast roaming. All APs of an APNetwork will use one same encrypt key. This encrypt key is randomly generated, and will be updated daily.

Link aggregation supports CAPWAP to improve WiFi performance (305156)

Link aggregation is used to combine multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain.

- FortiAP 320B and 320C models are supported.
- FortiAP 112B and 112D models **cannot** support link aggregation.
- NPI FAP-S3xxCR and "wave2" FAP/FAP-S models will have link aggregation feature via synchronization with regular FortiAP trunk build.

Link aggregation can be set in the FortiAP's C LI. See FortiAP CLI for more information.

Blocking management access via non-management interface (307813)

Previously, FortiAP accepted Telnet and HTTP connection to any virtual interfaces that have an IP address. For security reasons, Telnet and HTTP access are now limited to br0 or br.vlan for AP_MGMT_VLAN_ID.

Support HTTPS and SSH administrative access for FortiAPs (355122)

FortiAP now supports HTTPS and SSH administrative access, as well as HTTP and Telnet.

CLI additions have been made under wtp-profile and wtp.

Syntax

```
config wireless-controller wtp-profile
   edit {profile}
      set allowaccess [telnet | http | https | ssh]
   end

config wireless-controller wtp
   edit 1
      set override-allowaccess [enable | disable]
      set allowaccess [telnet | http | https | ssh]
   end
```

Support to Disable PowerSave Feature (355273)

Added `transmit-optimize` under `wireless-controller wtp-profile` > `radio` to manually configure transmit optimization.

Syntax

```
config wireless-controller wtp-profile
   edit {profile}
      config {radio}
         set transmit-optimize [disable | power-save | aggr-limit | retry-limit | send-
             bar]
```

- **disable:** Disable transmit optimization.
- **power-save:** Mark a client as power save mode if excessive transmit retries happen.
- **aggr-limit:** Set aggregation limit to a lower value when data rate is low.
- **retry-limit:** Set software retry limit to a lower value when data rate is low.
- **send-bar:** Do not send BAR frame too often.

ARP not resolved for IPADs (364516)

Added the `arp-proxy` option under `config wireless-controller vap` > `set broadcast-suppression` to configure VAP to reply ARP requests for wireless clients as a proxy.

Option to block intra-SSID traffic in Bridge mode for client connected to same FortiAP (365128)

A FortiAP in Bridge mode can now block traffic to clients associated with same FortiAP. This is useful in hotspot deployments managed by a central FortiGate, but would also be useful in cloud deployments. Until now,this was only supported in Tunnel mode.

Run FortiAP shell command through CAPWAP control tunnel (365609)

Very often, the FortiAP in the field is behind a NAT device, and access to the FortiAP through Telnet or SSH is not available. As a troubleshooting enhancement, this feature allows an AP shell command up to 127-bytes sent to the FAP, and FAP will run this command, and return the results to the controller using the CAPWAP tunnel.

Maximal output from a command is limited to 4M, and the default output size is set to 32K.

The FortiAP will only report running results to the controller after the command is finished. If a new command is sent to the AP before the previous command is finished, the previous command will be canceled.

Syntax

```
diag w-c wlac wtpcmd wtp_ip wtp_port cmd [cmd-to-ap]
cmd: run,show,showhex,clr,r&h,r&sh
```

- **cmd-to-ap:** any shell commands, but AP will not report results until the command is finished on the AP
- **run:** controller sends the ap-cmd to the FAP to run
- **show:** show current results reported by the AP in text
- **showhex:** show current results reported by the AP in hex
- **clr:** clear reported results
- **r&s:** run/show
- **r&sh:** run/showhex

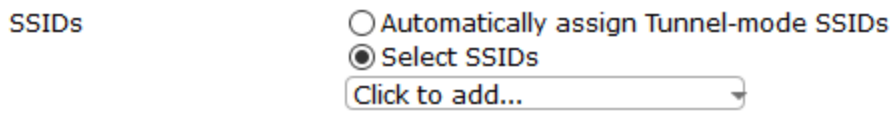
New Certificate Bundle 20160525 is available (373743)

A new WiFi certificate bundle is available, issued by Entrust. The chain is: wifi_cert > Entrust_L1K > Entrust_G2 > Entrust_Root.

Per Entrust's request, unpopular G2 root is removed from CA bundle.

Automatic all-SSID selection in FortiAP Profile (219347)

The SSID field in FortiAP Profiles now includes the option **Automatically assign Tunnel-mode SSIDs**. This eliminates the need to re-edit the profile when new SSIDs are created. You can still select SSIDs individually using the **Select SSIDs** option.



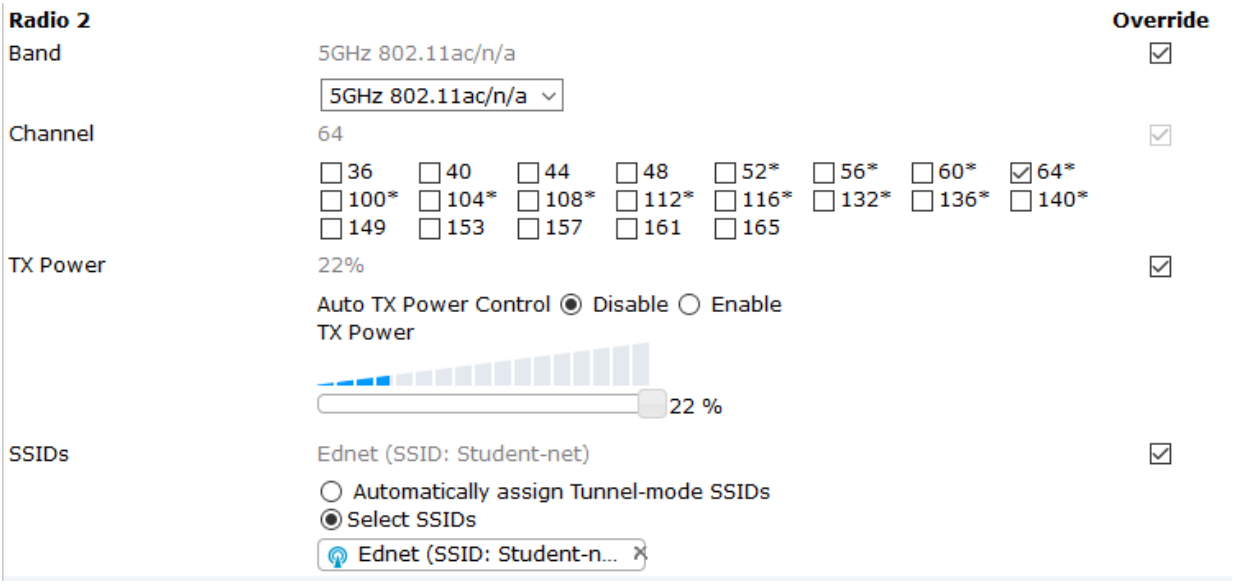
Automatic assignment of SSIDs is not available for FortiAPs in Local Bridge mode. The option is hidden on both the Managed FortiAP settings and the FortiAP Profile assigned to that AP.

Improved override of FortiAP settings (219347 264010 264897)

The configuration settings of a FortiAP in **WiFi Controller > Managed FortiAPs** can override selected settings in the FortiAP Profile:

- Band and/or Channel
- Transmitter Power
- SSIDs
- LAN Port mode

Note that a Band override also overrides Channel selections.



In the CLI, you can also override FortiAP LED state, WAN port mode, IP Fragmentation prevention method, spectrum analysis, and split tunneling settings.

Spectrum Analysis removed from FortiAP Profile GUI

Spectrum Analysis is no longer available in FortiAP Profiles in the GUI. It can be enabled in the CLI if needed.

Disable low data rates in 802.11a, g, n ac (297821)

To reduce air-time usage on your WiFi network, you can disable the use of low data rates which cause communications to consume more air time.

The 802.11 a, b, and g protocols are specified by data rate. 802.11a can support 6,9,12, 18, 24, 36, 48, and 54 Mb/s. 802.11b/g can support 1, 2, 5.5, 6, 9,12, 18, 24, 36, 48, 54 Mb/s. Basic rates are specified with the suffix "basic", "12-basic" for example. The capabilities of expected client devices need to be considered when deciding the lowest Basic rate.

The 802.11n and ac protocols are specified by MSC (Modulation and Coding Scheme) Index and the number of spatial streams.

- 802.11n with 1 or 2 spatial streams can support mcs0/1, mcs1/1, mcs2/1, mcs3/1, mcs4/1, mcs5/1, mcs6/1, mcs7/1,mcs8/2,mcs9/2, mcs10/2, mcs11/2, mcs12/2, mcs13/2, mcs14/2, mcs15/2.
- 802.11n with 3 or 4 spatial streams can support mcs16/3, mcs17/3, mcs18/3, mcs19/3, mcs20/3, mcs21/3, mcs22/3, mcs23/3, mcs24/4, mcs25/4, mcs26/4, mcs27/4, mcs28/4, mcs29/4, mcs30/4, mcs31/4.
- 802.11ac with 1 or 2 spatial streams can support mcs0/1, mcs1/1, mcs2/1, mcs3/1, mcs4/1, mcs5/1, mcs6/1, mcs7/1, mcs8/1, mcs9/1, mcs0/2, mcs1/2, mcs2/2, mcs3/2, mcs4/2, mcs5/2, mcs6/2, mcs7/2, mcs8/2, mcs9/2.
- 802.11ac with 3 or 4 spatial streams can support mcs0/3, mcs1/3, mcs2/3, mcs3/3, mcs4/3, mcs5/3, mcs6/3, mcs7/3, mcs8/3, mcs9/3, mcs0/4, mcs1/4, mcs2/4, mcs3/4, mcs4/4, mcs5/4, mcs6/4, mcs7/4, mcs8/4, mcs9/4

Here are some examples of setting basic and supported rates.

```
config wireless-controller vap
   edit <vap_name>
      set rates-11a 12-basic 18 24 36 48 54
      set rates-11bg 12-basic 18 24 36 48 54
      set rates-11n-ss34 mcs16/3 mcs18/3 mcs20/3 mcs21/3 mcs22/3 mcs23/3 mcs24/4 mcs25/4
      set rates-11ac-ss34 mcs0/3 mcs1/3 mcs2/3 mcs9/4 mcs9/3
   end
```

WiFi and Switch controllers are enabled separately (275860)

In the Feature Store (**System > Features**), the WiFi Controller and Switch Controller are now separate. However, the Switch Controller must be enabled in order for the WiFi Controller to be visible.

In the CLI, the settings that enable the WiFi and Switch controllers have been separated:

```
config system global
   set wireless-controller enable
   set switch-controller enable
end
```

The settings that enable the GUI display for those controllers have also been separated:

```
config system settings
   set gui-wireless-controller enable
   set gui-switch-controller enable
end
```

Add Support of LLDP protocol on FortiAP to send switch and port information (283107)

You can enable LLDP protocol in the FortiAP Profile. Each FortiAP using that profile can then send back information about the switch and port that it is connected to. This information is visible in the optional LLDP column of the Managed FortiAP list. To enable LLDP:

```
config wireless-controller wtp-profile
   edit <profile-name>
      set lldp enable
   end
```

WTP groups (278462)

You can define FortiAP Groups. Each group can contain FortiAPs of a single platform (model). These groups can be used in VLAN-pooling to assign APs to particular VLANs. Create a FortiAP Group in the CLI like this:

```
config wireless-controller wtp-group
   edit 1
      set platform-type 320C
      config wtp-list
         edit FP320C3X14010828
         next
         edit FP320C3X14010830
         end
      end
```

The `platform-type` field is optional. If it is left empty, the group can contain FortiAPs of any model.

VLAN-pooling (278462)

In an SSID, you can define a VLAN pool. As clients associate to an AP, they are assigned to a VLAN. A VLAN pool can

- assign a specific VLAN based on the AP's FortiAP Group, usually for network configuration reasons, or
- assign one of several available VLANs for network load balancing purposes (tunnel mode SSIDs only)

Assignment by FortiAP Group

In this example, VLAN 101, 102, or 103 is assigned depending on the AP's FortiAP Group.

```
config wireless-controller vap
   edit wlan
      set vlan-pooling wtp-group
      config vlan-pool
         edit 101
            set wtp-group wtpgrp1
         next
         edit 102
            set wtp-group wtpgrp2
         next
         edit 103
            set wtp-group wtpgrp3
         end
      end
```

Load Balancing

The vlan-pooling type can be either of these:

- **round-robin** - from the VLAN pool, choose the VLAN with the smallest number of clients
- **hash** - choose a VLAN from the VLAN pool based on a hash of the current number of SSID clients and the number of entries in the VLAN pool

If the VLAN pool contains no valid VLAN ID, the SSID's static VLAN ID setting is used.

In this example, VLAN 101, 102, or 103 is assigned using the round-robin method:

```
config wireless-controller vap
   edit wlan
      set vlan-pooling round-robin
      config vlan-pool
         edit 101
         next
         edit 102
         next
         edit 103
      end
   end
```

Option to disable automatic registration of unknown FortiAPs (272368)

By default, FortiGate adds newly discovered FortiAPs to the Managed FortiAPs list, awaiting the administrator's authorization. Optionally, you can disable this automatic registration function. A FortiAP will be registered and listed only if its serial number has already been added manually to the Managed FortiAPs list. AP registration is configured on each interface. Disable automatic registration in the CLI like this:

```
config system interface
   edit port15
      set ap-discover disable
   end
```

Automatic authorization of extension devices

To simplify adding FortiAP or FortiSwitch devices to your network, you can enable automatic authorization of devices as they are connected, instead of authorizing each one individually. This feature is available only on network interfaces designated as Dedicated to Extension Device.

To enable automatic authorization on all dedicated interfaces

```
config system global
   set auto-auth-extension-device enable
end
```

To enable automatic authorization per-interface

```
config system interface
   edit port15
      set auto-auth-extension-device enable
   end
```

In the GUI, the **Automatically authorize devices** option is available when **Addressing Mode** is set to **Dedicated to Extension Device**.

Control WIDS client deauthentication rate for DoS attack (285674 278771)

As part of mitigating a Denial of Service (DoS) attack, the FortiGate sends deauthentication packets to unknown clients. In an aggressive attack, this deauthentication activity can prevent the processing of packets from valid clients. A new WIDS Profile option in the CLI limits the deauthentication rate.

```
config wireless-controller wids-profile
   edit default
```

```
      set deauth-unknown-src-thresh 10
   end
```

The range is 1 to 65,535 deathorizations per second. 0 means no limit. The default is 10.

Prevent DHCP starvation (285521)

The SSID broadcast-suppression settings in the CLI now include an option to prevent clients from depleting the DHCP address pool by making multiple requests. Add this option as follows:

```
config wireless-controller vap
   edit "wifi"
      append broadcast-suppression dhcp-starvation
   end
```

Prevent ARP Poisoning (285674)

The SSID broadcast-suppression settings in the CLI now include an option to prevent clients from spoofing ARP messages. Add this option as follows:

```
config wireless-controller vap
   edit "wifi"
      append broadcast-suppression arp-poison
   end
```

Suppress all other multicast/broadcast packets (282404)

The SSID broadcast-suppression field in the CLI contains several options for specific multicast and broadcast packet types. Two new options suppress multicast (mc) and broadcast (bc) packets that are not covered by any of the specific options.

```
config wireless-controller vap
   edit "wifi"
      append broadcast-suppression all-other-mc all-other-bc
   end
```

A new configurable timer flushes the wireless station presence cache (283218)

The FortiGate generates a log entry only the first time that station-locate detects a mobile client. No log is generated for clients that have been detected before. To log repeat client visits, previous station presence data must be deleted (flushed). The sta-locate-timer can flush this data periodically. The default period is 1800 seconds (30 minutes). The timer can be set to any value between 1 and 86400 seconds (24 hours). A setting of 0 disables the flush, meaning a client is logged only on the very first visit.

The timer is one of the wireless controller timers and it can be set in the CLI. For example:

```
config wireless-controller timers
   set sta-locate-timer 1800
end
```

The sta-locate-timer should not be set to less than the sta-capability-timer (default 30 minutes) because that could cause duplicate logs to be generated.

Distributed Automatic Radio Resource Provisioning (DARRP) support (283501)

Through DARRP, each FortiAP unit autonomously and periodically determines the channel that is best suited for wireless communications. The distributed ARRP feature allows FortiAP units to select their channel so that they do not interfere with each other in large-scale deployments where multiple access points have overlapping radio ranges. Furthermore, Fortinet's implementation of DARRP simplifies operations by removing dependency on client software or hardware.

By default, DARRP optimization occurs at a fixed interval of 1800 seconds. Optionally, you can now schedule optimization for a fixed time. This enables you to confine DARRP activity to a low-traffic period. Setting `darrp-optimize` to 0, makes `darrp-day` and `darrp-time` available. For example, here's how to set DARRP optimization for 3:00am every day:

```
config wireless-controller timers
   set darrp-optimize 0
   set darrp-day sunday monday tuesday wednesday thursday friday saturday
   set darrp-time 03:00
end
```

Both `darrp-day` and `darrp-time` can accept multiple entries.

The FAP-320C, 320B and 112B second WAN port can be configured as a LAN bridge (261415)

This change makes FortiAP models 320C, 320B and 112B work more like other FortiAP models with LAN ports. The LAN port can be

- bridged to the incoming WAN interface
- bridged to one of the WiFi SSIDs that the FortiAP unit carries
- connected by NAT to the incoming WAN interface

The LAN port is labeled LAN2. The port labeled LAN1 acts as a WAN port connecting the FortiAP to a FortiGate or to FortiCloud. By default, LAN2 is bridged to LAN1. Access to other modes of LAN2 operation must be enabled in the CLI:

```
config wireless-controller wtp-profile
   edit <profile_name>
      set wan-port-mode wan-lan
   end
```

By default `wan-port-mode` is set to `wan-only`.

When `wan-port-mode` is set to `wan-lan`, LAN2 Port options are available in the FortiAP Profile, the same as other FortiAP models with LAN ports, such as 11C and 14C. In the GUI, see the **LAN Port** settings in **Wireless Controller > FortiAP Profiles**. In the CLI, use the `config lan` subcommand of `config wireless-controller wtp-profile`. LAN Port settings can be overridden on individual FortiAPs.

The WAN port can also be configured on the FortiAP's CLI. See FortiAP CLI for more information.

SSID Groups (264010)

SSID groups have SSIDs as members and can be used just like an individual SSID. To create an SSID group go to **WiFi Controller > SSID** and select **Create New > SSID Group**. An SSID can belong to multiple groups.

GUI improvements (205523 278771 278898)

- Managed FortiAP pages now show WTP Mode, either Normal or Remote. WTP Mode is an optional column in the Managed FortiAPs list.
- WIDS Profile is an optional column in the FortiAP Profiles list.
- If a software switch interface contains a SSID (but only one), the WiFi SSID settings are available in the switch interface settings.

CAPWAP Protected Management Frames (PMF) support (244510)

Protected Management Frames protect some types of management frames like deauthorization, disassociation and action frames. This feature, now mandatory on WiFi certified 802.1ac devices, prevents attackers from sending plain deauthorization/disassociation frames to disrupt or tear down a connection/association. PMF is a Wi-Fi Alliance specification based on IEEE 802.11w.

PMF is configurable only in the CLI.

```
config wireless-controller vap
   edit <vap_name>
      set pmf {disable | enable | optional}
      set pmf-assoc-comeback-timeout <integer>
      set pmf-sa-query-retry-timeout <integer>
      set okc {disable | enable}
   next
end
```

`optional` Enable PMF and allow clients without PMF.

`pmf-assoc-comeback-timeout` Protected Management Frames (PMF) maximum timeout for comeback (1-20 seconds).

`pmf-sa-query-retry-timeout` Protected Management Frames (PMF) sa query retry timeout interval (in 100 ms), from 100 to 500. Integer value from 1 to 5.

`okc` enable or disable Opportunistic Key Caching (OKC).

Opportunistic Key Caching Support (244510)

To facilitate faster roaming client roaming, you can enable Opportunistic Key Caching (OKC) on your WiFi network. When a client associates with an AP, its PMK identifier is sent to all other APs on the network. This eliminates the need for an already-authenticated client to repeat the full EAP exchange process when it roams to another AP on the same network.

OKC is configurable only in the CLI.

```
config wireless-controller vap
   edit <vap_name>
      set okc {disable | enable}
   next
end
```

FortiPresence push REST API (273954)

When the FortiGate is located on a private IP network, the FortiPresence server cannot poll the FortiGate for information. Instead, the FortiGate must be configured to push the information to the FortiPresence server.

The configuration parameters are:

fortipresence-server	FortiPresence server IP address
fortipresence-port	FortiPresence server UDP listening port (the default is 3000)
fortipresence-secret	FortiPresence secret password (8 characters maximum)
fortipresence-project	FortiPresence project name (16 characters maximum)
fortipresence-frequency	FortiPresence report transmit frequency (Range 5 to 65535 seconds. Default = 30)
fortipresence-rogue	Enable/disable FortiPresence reporting of Rogue APs
fortipresence-unassoc	Enable/disable FortiPresence reporting of unassociated devices

For example,

```
config wireless-controller wtp-profile
   edit "FP223B-GuestWiFi"
      config lbs
         set fortipresence enable
         set fortipresence-server 10.10.0.1
         set fortipresence-port 3000
         set fortipresence-secret "hardtoguess"
         set fortipresence-project fortipresence
         set fortipresence-frequency 30
         set fortipresence-rogue : disable
         set fortipresence-unassoc: disable
      end
```

More detailed information will be provided in FortiPresence documentation.

GUI support for WiFi SSID schedules (276425 269695 269668)

WiFi SSIDs include a schedule that determines when the WiFi network is available. The default schedule is Always. You can choose any schedule (but not schedule group) that is defined in **Policy & Objects > Objects > Schedules**.

CLI Syntax

```
config wireless-controller vap
   edit vap-name
      set schedule always
   end
```

The WiFi SSID list includes a Schedule column.

SSID Groups

An SSID Group has SSIDs as members and can be specified in any field that accepts an SSID.

To create an SSID Group in the GUI, go to **WiFi Controller > SSID** and select **Create New > SSID Group**. Give the group a **Name** and choose **Members** (SSIDs, but not SSID Groups).

To create an SSID Group in the CLI:

```
config wireless-controller vap-group
   edit vap-group-name
      set vaps "ssid1" "ssid2"
   end
```

RADIUS Change of Authorization (CoA) support

The CoA feature enables the FortiGate to receive a client disconnect message from the RADIUS server. This is used to disconnect clients when their time, credit or bandwidth had been used up. Enable this on the RADIUS server using the CLI:

```
config user radius
   edit <server_name>
      set radius-coa enable
   end
```

CAPWAP offloading to NPU

On FortiGates with the NP6 processor, offloading of CAPWAP traffic to the NP6 is enabled by default.

Administrative access to managed FortiAPs

By default, telnet access to a FortiAP unit's internal configuration is disabled when the FortiAP is managed (has been authorized) by a FortiGate. You can enable administrative access in the FortiAP profile, like this:

```
config wireless-controller wtp-profile
   edit FAP321C-default
      set allowaccess telnet
   end
```

The `allowaccess` field also accepts `http` to allow HTTP administatrative access.

The FortiAP Profile allowaccess settings can be overridden at the individual FortiAP:

```
config wireless-controller wtp
   edit FP321CX14004706
      set override-allowaccess enable
      set allowaccess telnet http
   end
```

Improved monitoring

The **WiFi Client Monitor** under **Monitor** displays top wireless user network usage and information that includes Device, Source IP, Source SSID, and Access Point. Disk logging must be enabled.

Wifi Clients and **Failed Authentication** views under **FortiView** are historical views.

FORTINET®

High Performance Network Security